LES FICHIERS DE POLICE ET DE GENDARMERIE

Alain Bauer
Christophe Soullez

puf

QUE SAIS-JE ?

Les fichiers de police et de gendarmerie

ALAIN BAUER

Professeur de criminologie au CNAM

CHRISTOPHE SOULLEZ

Criminologue

Deuxième édition mise à jour

3e mille

Introduction

En France, la tenue de fichiers de police est une pratique ancienne. Au Moyen Âge, le prévôt de Paris en charge de la justice et de la police royales pour Paris et sa banlieue, installé au Châtelet depuis le règne de Philippe-Auguste (1180-1223), fait tenir un registre des écrous.

L'année 1724 marque un tournant. Un décret du roi Louis XV crée ce qui semble être le premier registre centralisé à l'échelle de tout le Royaume. Tenu à l'Hôpital général des pauvres [1] de Paris et alimenté par tous les hôpitaux de province, il recense les mendiants arrêtés et fournit des renseignements sur leur identité, leur signalement, ainsi qu'une synthèse de leurs dépositions. Ce registre est communiqué, entre autres, aux officiers de la maréchaussée.

En 1752, cette mesure est généralisée à tous les « gibiers de police ». Le lieutenant général de police Berryer met en place le « livre rouge » et étend l'inscription aux registres aux individus arrêtés pour vols et autres crimes (sommiers judiciaires), aux personnes détenues par lettres de cachet [2] et enfin aux personnes de conduite suspecte (« ceux qui n'avaient pas d'autres ressources que l'intrigue ou fréquentaient de mauvaises compagnies »).

Parallèlement à l'évolution de l'organisation policière et aux missions de surveillance qui sont notamment confiées à la police parisienne en 1750, le traitement de l'information se professionnalise. Ainsi, Guillauté, officier de la maréchaussée, invente le premier système de stockage et de consultation des informations consignées sur des feuillets papiers par les officiers de police : le serre-papiers [3].

Initialement destinés à la répression et la surveillance des criminels récidivistes, les fichiers s'étendent progressivement à d'autres populations du fait de l'apparition de nouvelles formes d'incrimination (prostitution, vagabondage, etc.). À la fin du XIXe siècle, on recense déjà plusieurs fichiers : sommiers judiciaires ; fichier des interdits de séjour ; fichier des étrangers ; registre de la prostitution ; dossiers individuels de la section politique.

Dans leur organisation et leur forme, les fichiers évoluent fortement à partir de 1882, année au cours de laquelle la préfecture de Police, sous l'impulsion d'Alphonse Bertillon, se dote d'un service d'anthropométrie puis de photographie.

Différents scandales viendront émailler le développement des fichiers et notamment celui de l'affaire dite « des fiches » (1904), la mise en fiche de la population juive, des francs-maçons ou des homosexuels durant l'occupation.

Les fichiers, constitués de fichettes cartonnées, évoluent progressivement jusqu'à la fin des années 1960. Les fichettes tendent alors à être remplacées par des fichiers informatiques. En 1967, une mission procède à une inspection de la documentation policière. Pour la seule préfecture de police de Paris, elle recense près de 400 fichiers différents et 130 millions de fiches. Devant cette densité, un répertoire des fichiers doit même être édité par le ministère de l'Intérieur.

En 1975, la Commission « informatique et libertés », mise en place suite à la crise provoquée par le projet d'interconnexion de fichiers de police dénommé « SAFARI », tente de dresser une liste des différents fichiers existants et notamment ceux mis en œuvre par la police et la gendarmerie. La loi « Informatique et Libertés », votée en 1978, ouvrira la voie à la mise en place d'une réglementation protectrice des libertés et de la vie privée.

Quoi qu'il en soit, fichiers de police et Libertés individuelles sont usuellement opposés. La création, la modernisation ou encore l'extension des bases de données au sein de l'administration alimentent régulièrement le débat sur la protection du droit à la vie privée. Cela d'autant plus que les fichiers, qui ont souvent été cachés par les services de l'État au cours des siècles, font aujourd'hui l'objet d'une visibilité accrue du fait tant de la législation en vigueur obligeant à leur déclaration, que de la veille médiatique et associative.

Pourtant, pour protéger la population, et donc garantir les droits des individus à vivre en sécurité en retrouvant des criminels, il est essentiel de conserver, retraiter et rapprocher des informations. La mobilité des personnes et des flux et l'exigence de la preuve qui fonde l'État de droit rendent nécessaire le recours à des informations nominatives. Les systèmes informatiques des services de sécurité doivent également s'adapter aux structures sociales, aux mutations technologiques mais également aux évolutions des groupes criminels ou terroristes qui sont aussi les premiers utilisateurs des nouvelles technologies.

Il faut donc veiller à l'équilibre entre le développement des fichiers et leur indispensable contrôle par des magistrats et des autorités indépendantes, et ceci, d'ailleurs, pour tous les fichiers, qu'ils soient policiers, couverts par le secret ou gérés par d'autres administrations que la police et la gendarmerie.

Avec la puissance croissante de l'informatique, avec la multiplication des traces numériques que nous laissons quotidiennement sous toutes les formes (et donc la difficulté de les effacer et de corriger les erreurs), c'est à un véritable basculement de société que nous assistons. Le développement des réseaux sociaux du Web 2.0 alimente paradoxalement cette inquiétude alors même que chacun y délivre volontairement des informations personnelles qu'il serait impensable de stocker dans des fichiers administratifs. Ce qui pouvait donc auparavant passer pour une question secondaire devient aujourd'hui un enjeu de société.

Notes

[1] Cet hôpital a été créé par un édit royal de 1656. Tous les mendiants de Paris doivent s'y présenter spontanément pour y être enfermés, sous peine de sanctions (fouet ou galères en cas de récidive).
[2] Les lettres de cachet sont des lettres fermées signées du roi. Elles contiennent le plus souvent un ordre individuel d'exil ou d'emprisonnement, ou encore d'internement. Cette institution permet d'arrêter rapidement un suspect, de réprimer un délit de presse, surtout de mettre à l'écart un fils de famille indigne, débauché ou prodigue : Sade et Mirabeau furent les plus célèbres « victimes » de cet usage.
[3] M. Guillauté, *Mémoire sur la réformation de la police en France*, Paris, 1749, rééd. Hermann, 1974.

Chapitre I

Des fichiers, pour quelles finalités ?

I. Qu’est-ce qu’un fichier ?

Le mot « fichier » ne s’impose qu’avec l’apparition du « bertillonnage » [1] en 1870. Avant, on parlait de registres, de sommier, etc. Les fichiers se sont développés parallèlement à l’évolution de l’organisation de l’État, lorsqu’il s’est agi de créer des archives, d’établir des catalogues, des répertoires, des inventaires, donc de classer, d’ordonner, de ranger pour mieux connaître, pour mieux voir et pour mieux gérer. Au Moyen Âge, les registres paroissiaux sont d’ailleurs les tout premiers fichiers créés en vue de mieux connaître la population.

Le développement des herbiers sous l’Ancien Régime a sûrement permis à l’institution policière, alors en pleine professionnalisation, de mieux contrôler les populations maintenues sous surveillance. C’est sous le Consulat et l’Empire, et notamment sous l’impulsion de Fouché, que le recueil d’informations va s’ériger en système. Entre les biographies ou topographies chouanniques et les bulletins envoyés quotidiennement par le ministère de la Police à Napoléon, l’écriture et le renseignement sont placés au cœur de l’appareil d’État.

Le décret impérial du 25 mars 1811 a créé les premiers « commissaires spéciaux » attachés à la surveillance de l’opinion dont les attributions sont de « surveiller particulièrement l’esprit public des habitants, les opérations de commerce et celles de la conscription, le service des douanes, le mouvement des ports, la ligne des côtes et des frontières, les communications avec l’étranger, les subsistances, la librairie, l’instruction publique, les associations politiques et religieuses et, en général, toutes les parties de l’administration et des services publics ». Cette police « spéciale » fut supprimée sous la Restauration. Le terme ne devait réapparaître qu’en novembre 1846 dans une ordonnance royale

prévoyant la création de « commissaires spéciaux des chemins de fer », ancêtres des renseignements généraux. La création de ces services est allée de pair avec le développement des dispositifs de fichage portant, notamment, sur les éventuels opposants au régime qui se déplaçaient sur le territoire national en utilisant les nouvelles voies de transports.

La mise en fiche de la population a, par ailleurs, pris un nouveau tournant lors de l'institution de la statistique morale et personnelle de la nation en 1807 : dans tous les départements, les fonctionnaires du ministère de la Police sont alors chargés de dresser un tableau de la population, relever l'histoire personnelle de chaque habitant et enregistrer des renseignements concernant leur patrimoine, leur moralité et leurs opinions.

À cette frénésie de fichage de la police impériale, qui concerne l'ensemble du corps social, succède, avec la création de la police technique, la professionnalisation du traitement de l'information dont le recueil ne concerne plus que les individus considérés comme « dangereux ».

L'arrivée de l'informatique dans les années 1980 bouleverse la manière de traiter l'information. Elle donne surtout un coup d'accélérateur aux nombreux projets visant à centraliser, rationaliser et mieux exploiter la documentation policière. Au milieu des années 1980, il est ainsi question de développer « l'exploitation optimale des éléments contenus dans les procédures policières en rendant ces informations directement accessibles aux utilisateurs, sans qu'il leur soit nécessaire de sortir ou de consulter les documents archivés. Pour parvenir à cette solution, il faut développer l'importance du contenu des fichiers au détriment des manipulations et mettre en place un système d'autorégulation des dossiers permettant une actualisation permanente des documents les plus intéressants et une expurgation progressive des dossiers de moindre valeur » [2]. Il s'agit donc de simplifier l'accès à l'information et de lui donner un sens, à travers la qualité des données enregistrées, en vue d'une exploitation ciblée.

En ce qui concerne le cadre législatif, il a fallu attendre la loi du 6 janvier 1978 (voir encadré ci-dessous) pour avoir la première définition légale de ce qu'est un fichier ou plutôt un « traitement de données nominatives », ainsi que la première réglementation de leur usage tant en ce qui concerne leur création, la nature des informations susceptibles d'être enregistrées, leur statut ou leur contrôle. Vient ensuite la loi du 7 août 1985, dite de modernisation de la Police nationale, qui a permis à la police de rattraper son retard en matière de police technique et

scientifique, notamment dans le domaine de l'informatisation des grands fichiers de recherche.

Le terme « fichier », comme l'outil lui-même, est utilisé quotidiennement. La plupart des personnes physiques ou morales disposent d'un ou de plusieurs fichiers pouvant contenir des informations plus ou moins variables. Ainsi, chacun possède un répertoire téléphonique incluant nom, prénom, adresse, téléphone et adresse courriel. Les entreprises créent et développent des fichiers sur leurs personnels, leurs clients, leurs fournisseurs. L'État et les administrations conçoivent, modernisent, étendent leurs bases de données afin d'améliorer leur productivité, de mieux servir les usagers ou en vue de renforcer l'efficacité du service rendu au public.

Loi du 6 janvier 1978 (art. 1er)

L'informatique doit être au service de chaque citoyen. Son développement doit s'opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l'identité humaine, ni aux droits de l'homme, ni à la vie privée, ni aux libertés individuelles ou publiques.

La présente loi s'applique aux traitements automatisés de données à caractère personnel, ainsi qu'aux traitements non automatisés de données à caractère personnel contenues ou appelées à figurer dans des fichiers, à l'exception des traitements mis en œuvre pour l'exercice d'activités exclusivement personnelles.

La loi du 6 août 2004, qui transpose la directive européenne 95/46 ce du 24 octobre 1995 sur la protection des personnes physiques à l'égard du traitement des données à caractère personnel et à la libre circulation des données, a remanié la loi « Informatique et Libertés » de 1978. La notion de « données à caractère personnel » s'est substituée à celle d'« informations nominatives ». La nouvelle loi propose donc une définition plus large de ce qui est considéré comme une information susceptible d'être visée par la réglementation sur les fichiers.

Aujourd'hui, au sens de la loi, constitue une « donnée à caractère personnel » toute information relative à une personne physique identifiée ou qui peut être identifiée, directement ou indirectement, par référence à un numéro

d’identification ou à un ou plusieurs éléments qui lui sont propres. Pour déterminer si une personne est identifiable, il convient de considérer l’ensemble des moyens en vue de permettre son identification dont dispose ou auxquels peut avoir accès le responsable du traitement ou une autre personne. Cette définition concerne aussi les traitements qui, bien que ne comportant pas de noms de personnes, peuvent cependant permettre de les identifier indirectement, que ce soit par l’indication de leur numéro de Sécurité sociale, l’insertion d’une photographie ou encore par le rapprochement de données.

Constitue un traitement de données à caractère personnel toute opération ou tout ensemble d’opérations portant sur de telles données, quels que soient le procédé utilisé, et notamment la collecte, l’enregistrement, l’organisation, la conservation, l’adaptation ou la modification, l’extraction, la consultation, l’utilisation, la communication par transmission, diffusion ou toute autre forme de mise à disposition, le rapprochement ou l’interconnexion, ainsi que le verrouillage, l’effacement ou la destruction.

II. La nécessaire adaptation des outils policiers

Les fichiers sont aussi vieux que l’écriture, car l’écriture est la meilleure des mémoires, plus sûre et plus pérenne que la mémoire humaine. Il est donc logique que dès l’émergence d’une fonction policière, et surtout à partir du moment où celle-ci s’est autonomisée par rapport au pouvoir politique, le recours à la pratique du fichage se soit très vite imposé.

Rappelons cependant que les premiers fichiers utiles aux forces de l’ordre – et ils le sont encore – ne sont pas des fichiers policiers, ni même d’essence politique. Ce sont les registres d’état civil, tenus d’abord par l’Église (et que François Ier uniformise), puis par l’État et les collectivités territoriales. C’est ainsi dans un deuxième temps que le pouvoir temporel a compris l’intérêt de maîtriser, et donc de contrôler, cette fonction d’enregistrement des principales étapes (naissance, mariage, décès) de la vie de chaque individu, qui donne accès à des informations précieuses sur les populations (filiation, parenté, lieu d’origine, migration géographique, etc.).

Les fichiers policiers se sont créés ensuite, sur des initiatives locales ou sur instruction du pouvoir central, pour rassembler d'autres informations utiles collectées à l'occasion de missions policières (parcours judiciaire des délinquants, surveillance politique des opposants, mesures de prophylaxie à l'égard de certains milieux comme les prostituées).

Avec le progrès technique et scientifique, la masse d'informations utiles a augmenté, de même que les moyens de communication et de stockage de l'information se sont perfectionnés. Parallèlement, la découverte des premiers moyens modernes d'identification criminologique (la photographie, l'anthropométrie judiciaire ou « système Bertillon », les empreintes digitales) a changé la nature des informations contenues dans les fichiers de police. Et que dire de la découverte de l'adn, qui a complètement révolutionné l'approche des enquêtes de police et amené la création d'un nouveau fichier génétique ?

Ce développement des fichiers ne résulte pas seulement sur un simple accroissement des fichiers de police, tel que le supposent l'opinion publique et les médias, mais souvent aussi sur une modernisation ou une adaptation de ceux-ci, tant à l'environnement technologique que législatif.

Ainsi, la modernisation du service public fait automatiquement basculer dans le champ de compétence de la Commission nationale de l'informatique et des libertés (cnil) des pans croissants de l'activité des services de police et de gendarmerie. Juridiquement, la loi « Informatique et Libertés » du 6 janvier 1978 s'applique indistinctement aux fichiers manuels et aux fichiers numérisés. Mais la tendance à l'informatisation de procédures qui préexistaient, soit de manière informelle, soit organisées autour d'une consignation écrite sur de simples registres, aboutit nécessairement à la remise à plat, et donc à la déclaration, de nouveaux fichiers informatiques. Dans ce cas, la création d'un fichier ne correspond pas à une véritable extension du « fichage » si ce n'est que l'outil informatique est porteur de fonctionnalités nouvelles. En outre, les formalités préalables à l'autorisation d'un fichier imposent un exercice d'explicitation et de hiérarchisation des finalités poursuivies, de justification de la proportionnalité et de déploiement de mesures de protection de la confidentialité des informations, autant de garanties imposées par la loi de 1978. La cnil veille très précisément à cette dimension et exige, concomitamment à l'examen du projet d'autorisation, un dossier administratif et technique très détaillé.

La modernisation des fichiers sert aussi à accroître l'efficacité de la lutte contre

la délinquance. La meilleure connaissance des individus, de leurs relations et de leurs pratiques criminelles permet d'obtenir de meilleurs résultats, grâce à une prévention plus efficace et une répression plus ciblée. Mais la lutte entre les policiers et les délinquants est une course contre la montre : plus la police est efficace, plus cela incite les criminels à changer leurs méthodes, leurs fréquentations, rendant ainsi obsolètes les informations contenues dans les fichiers.

Les criminels et les délinquants sont aussi des utilisateurs des nouvelles technologies. Soit qu'ils s'en servent comme moyen de commettre, selon des modes opératoires renouvelés, des infractions connues de longue date (on peut évoquer à titre d'exemple la pédopornographie ou l'escroquerie sur Internet). Soit que la dépendance croissante de nos sociétés envers les systèmes interconnectés de communications électroniques constitue une vulnérabilité jusqu'alors inconnue. Toute menace crédible d'atteinte à l'intégrité de ces réseaux confère un poids et un impact criminels très fort à ses auteurs (chantages ou menaces, terrorisme).

La téléphonie mobile et l'Internet offrent une furtivité et une capacité d'organisation sans précédent aux délinquants. Leur surveillance est d'une complexité redoutable à organiser, beaucoup plus que celle de la voie publique. Aussi, les nouveaux outils juridiques ou technologiques mis à disposition des services de police et de gendarmerie correspondent davantage à une mise à niveau et à une adaptation des services de sécurité intérieure aux nouvelles réalités économiques et sociales qu'à un empiétement supplémentaire de la sphère étatique sur la sphère privée. Ainsi, par exemple, l'Office central des nouvelles technologies de l'information et de la communication qui traque la cybercriminalité en adressant des réquisitions judiciaires aux opérateurs de communications électroniques n'est jamais que l'équivalent appliqué à Internet des « Brigades du Tigre » créées voici un siècle pour lutter contre les bandes armées circulant en automobile.

Les modalités de l'action policière, et par conséquent les sources d'information des policiers, évoluent avec les structures sociales non seulement au niveau national, mais aussi au niveau international. Les fichiers de police s'adaptent à l'évolution du monde, à l'internationalisation de la criminalité, anciennes ou nouvelles mafias qui se jouent aussi bien des frontières que des États. La souplesse des organisations criminelles, leur appât pour le gain, leur détermination leur ont donné une avance indéniable sur la réponse policière qui

s’est heurtée – et qui se heurte toujours – aux carcans bureaucratiques, de la diplomatie, de la politique et des intérêts nationaux. Ainsi, il a fallu attendre bien longtemps avant la création de fichiers internationaux (ex. : celui d’Interpol, organisation créée en 1923) abondés par les renseignements fournis volontairement par les États adhérents à l’organisation et mis en commun.

III. Informer le Gouvernement

On peut raisonnablement supposer, bien qu’il n’en reste pas de traces, que des fichiers à dimension politique ont existé bien avant les premiers fichiers policiers. En effet, il n’y a pas de bon gouvernement sans une information fiable, car comme le dit Émile de Girardin, « gouverner, c’est prévoir ».

Ce qu’on appelle l’information du Gouvernement, c’est aussi bien l’information stratégique qui permet d’anticiper les mouvements sociaux, l’information institutionnelle qui caractérise ses interlocuteurs dans leurs fonctions et leur histoire, mais aussi, même si c’est moins avouable, des informations plus personnelles concernant la respectabilité et le passé des individus.

Dans le monde, et notamment en France, tous les régimes ont eu – ou ont encore aujourd’hui – leur police politique, parfois de sinistre réputation, exerçant dans la clandestinité. Dans le domaine du renseignement, la limite entre le recueil de l’information opérationnelle et celui à vocation plus « politique » n’est pas toujours très claire. Il n’y a pas d’autres garde-fous que la conscience des gouvernants et le sens civique des exécutants, tant l’extension de la notion de sécurité nationale peut parfois tout recouvrir, de son absence de justification à l’opacité du « secret d’État ».

Pour autant, faut-il dénier à un gouvernement légitime et démocratique le droit de disposer des moyens normaux de renseignement et d’anticipation ? Doit-on interdire à un gouvernement des pratiques que l’on tolère de la part de sociétés privées ou que l’on retrouve librement sur les réseaux dits sociaux de l’Internet, comme Facebook ?

Dans la mesure où l’on demande à un gouvernement de rendre compte de ses agissements, de ses prises de parole et de ses fréquentations, n’est-il pas normal qu’il dispose des moyens de se renseigner. Ne serait-ce que parce qu’on lui reprocherait avec autant de véhémence de ne pas l’avoir fait, par exemple, après

un attentat ?

Il ne s’agit pas, bien sûr, de restaurer des pratiques d’un autre âge qui consisteraient à faire pression sur les individus, mais il est logique qu’une autorité publique sache, avant de recevoir un interlocuteur, s’il est aussi représentatif qu’il le prétend et, surtout, si la moralité publique de cette personne n’expose pas la puissance invitante à des risques, voire à un scandale. Et que dire d’un recrutement sensible pour un responsable d’installation nucléaire ou d’un service de renseignement ? Cette observation vaut également pour les délégués territoriaux du Gouvernement que sont les préfets. Parce qu’ils sont les représentants de l’intérêt général, parce qu’on exige d’eux des agissements sans faille, il est normal qu’on contrôle leur situation avant de leur donner accès à certaines informations sensibles.

De même, le Gouvernement, chargé d’assurer l’ordre public, doit pouvoir être informé des manifestations publiques pouvant avoir des conséquences sur la circulation ou sur la sécurité des personnes et des biens. Il a donc besoin de connaître ses éventuels interlocuteurs, les personnes qui, au sein d’une organisation associative, sociale ou syndicale, ont des capacités à négocier et à peser sur les choix de l’organisation et de ses membres. Comme il lui est indispensable, sur un territoire, de pouvoir disposer d’une vision globale des principaux acteurs institutionnels. Mais les informations dont il doit alors disposer ne doivent bien entendu porter que sur des faits utiles à sa mission et non sur des données relevant de la vie privée comme, par exemple, le comportement sexuel ou la santé des intéressés.

Souvent, les informations dont disposent les préfets sont, pour la plupart, recueillies en milieu ouvert, dans les journaux ou sur Internet maintenant. Mais, afin d’éviter, à chaque fois que nécessaire, de rechercher ces informations, elles font l’objet d’un enregistrement dans un fichier qui peut être consulté plus facilement et qui doit faire l’objet d’une déclaration. Ainsi, ce type de fichiers peut faire l’objet de contrôles, quand les fichiers manuels ne laissaient aucune trace.

IV. Aider à la résolution des enquêtes

La Police et la Gendarmerie nationales ont deux missions principales : la prévention des crimes et délits, qui s’apparente aux missions de police

administrative, et la recherche des auteurs d'infractions, qui relève de la police judiciaire.

Pour agir efficacement en matière policière, il faut conserver, retraiter et rapprocher des informations. Certes, on peut déjà travailler à partir de données agrégées et anonymes, telles que la répartition cartographique et temporelle des plaintes déposées ou des événements de voie publique enregistrés. Mais cela est très insuffisant face à la mobilité des personnes et des flux qui sont la marque de notre société. Et ce ne peut être une réponse à l'exigence du rapport de la preuve de nos États de droit.

À défaut de ces informations, on s'en remettrait trop exclusivement à la part de contingence que recèle inévitablement la présence concomitante sur les lieux de l'infraction d'une patrouille. Au-delà des efforts à accomplir pour mieux répartir la présence policière en coïncidence avec la réalité criminogène dans l'espace et dans le temps, il sera toujours impossible de garantir la présence d'un policier ou d'un témoin irrécusable et disposé à témoigner sur les lieux de chaque infraction. Pour lutter contre l'impunité, police et gendarmerie ne peuvent agir sans mémoire, sans fichiers d'identification, sans accès aux dispositifs technologiques qui conservent la trace des actions humaines dans une société urbanisée développée.

La maîtrise du dernier état de l'art de la police scientifique et l'existence de fichiers opérationnels, complets et consultables en temps réel, sont assurément nécessaires pour que ces missions puissent être remplies avec efficacité et rapidité et permettant d'éviter l'éventuelle récidive de l'auteur d'une infraction.

L'activité de police ne saurait pour autant se fier aveuglément et intégralement à des traitements automatisés de données. La dimension humaine, voire psychologique, devra toujours rester un axe cardinal de l'action policière. L'empathie avec le plaignant ou la victime, outre qu'elle constitue une obligation morale et un soutien indispensable pour surmonter le traumatisme de l'agression, permet aussi de recueillir des indices utiles à l'enquête. Aucun traitement automatisé ne saurait suppléer le sens de l'initiative, le « flair », sans lesquels bien des affaires résolues en flagrant délit seraient manquées. Le raisonnement hypothético-déductif qui structure toute enquête, le recueil et la synthèse du renseignement opérationnel relatif à un risque ou une menace pas toujours précisément identifiés ou encore l'analyse de proportionnalité qui sous-tend la police administrative renvoient irréductiblement à l'exercice des facultés

de jugement et de discernement du policier.

Mais, il est pourtant évident qu'il existe une nette corrélation entre la modernisation accélérée des fichiers de police et l'amélioration du taux d'élucidation des affaires.

La lutte contre la criminalité n'est pas une science exacte. Une information, matériau de base de l'enquête policière, administrative ou judiciaire, a une fiabilité plus ou moins grande, selon qu'elle a été vérifiée, recoupée, ou non, selon qu'elle est ancienne ou qu'elle a fait l'objet d'une vérification récente. C'est l'un des objectifs des fichiers de police et de gendarmerie.

Les fichiers sont une mémoire. C'est l'accumulation des informations qu'ils contiennent qui les rend redoutables, à la fois en termes d'efficacité et en termes de possibilités d'erreurs (si l'information initiale en est entachée). À condition bien sûr que cette mémoire soit contrôlée, vérifiée, corrigée et expurgée le plus méthodiquement possible.

C'est cette mémoire compilée et démultipliée qui fait des fichiers un instrument incontournable des enquêtes judiciaires. Cela concerne évidemment les fichiers de police proprement dits, mais aussi toutes sortes de fichiers administratifs (fichier des permis de conduire, des cartes grises, etc.), voire privés (ex. : des fichiers bancaires ou toute autre trace informatique que chacun laisse quotidiennement derrière lui). La consultation peut concerner aussi bien des données ayant trait aux auteurs potentiels, mais aussi aux victimes, à leur entourage proche ou même à des témoins. Il s'agit, en effet, de vérifier ou d'infirmer des hypothèses, de comprendre le déroulement d'un scénario ou simplement de tracer le profil d'une victime.

Comme les autres instruments de l'enquête, la consultation des fichiers n'est qu'un outil au service de la vérité, et l'enquêteur ne doit jamais faire l'impasse sur une analyse critique de ces données, en se rappelant que toute information peut être erronée ou simplement absente du fichier. Toutes les informations recueillies en consultant un fichier doivent donc être mises en perspectives et vérifiées à la lumière des indices et des témoignages. Néanmoins, avec les progrès de l'informatique et l'amélioration des réseaux, tout individu laisse derrière lui de plus en plus d'empreintes numériques, qui sont autant d'éléments à analyser dans le cadre d'une enquête.

Au cours des enquêtes, certains fichiers (comme, par exemple, celui des empreintes génétiques – le fnaeg – dont la base s'enrichit quotidiennement) peuvent apparaître comme des armes absolues pour établir des preuves *quasi* irréfutables, et ils amènent effectivement à la résolution de très nombreuses affaires, parfois même en permettant de relier plusieurs affaires entre elles. D'autres fichiers semblent moins intéressants *a priori*, et seule la perspicacité (ou l'instinct) de l'enquêteur le conduira à penser à les consulter. Mais cette dimension de l'enquête prend chaque jour de l'ampleur : les fichiers sont aujourd'hui un point de passage obligé du processus d'enquête.

V. Contribuer à l'identification des auteurs d'actes criminels

Les principes fondateurs de la criminologie relèvent que l'intensité de l'acte délinquant est telle qu'il est rare que l'auteur d'une infraction ne laisse aucune marque de son passage sur la scène de l'acte commis, ou bien qu'il n'emporte sur lui ou ses vêtements aucune trace du milieu dans lequel il a agi. Ceci ouvre un vaste champ d'action à la police technique et scientifique qui n'a cessé de se développer, en suivant l'évolution de la science et des techniques modernes.

C'est à la fin du xixe siècle que le premier système moderne de police scientifique est mis en place par Alphonse Bertillon. Il fonde, en 1870, le laboratoire de police scientifique d'identification criminelle et invente un protocole de collecte des mensurations caractéristiques d'un individu, appelé « système Bertillon » ou « bertillonnage ». Ce système d'identification est rapidement adopté dans toute l'Europe, puis aux États-Unis.

C'est en 1882, à la préfecture de Police, lorsqu'il est chargé d'ordonnancer les dossiers sur des criminels notoires qu'il découvre qu'en prenant 14 mensurations (taille, pieds, main, nez, oreilles, etc.) sur n'importe quel individu, il n'y a qu'une seule chance sur 286 millions pour qu'on retrouve les mêmes chez une autre personne. Un matériel spécialisé va alors être utilisé dans tous les établissements pénitentiaires : table, tabouret, toise, compas de proportion, tablette et encreur pour prise d'empreintes digitales. Alphonse Bertillon n'est pas l'inventeur du système d'identification par empreintes digitales, l'inventeur concret de la technique dactyloscopique est Francis Galton. Toutefois, Bertillon

a été le premier à utiliser les empreintes digitales comme moyen d'identification lors de l'interpellation d'Henri-Léon Scheffer le 24 octobre 1902. C'est la première fois qu'un assassin fut identifié, convaincu de meurtre et condamné avec le recours à l'analyse des empreintes.

Depuis Bertillon, la science a fait d'énormes progrès qui se traduisent par de nouveaux outils d'aide à l'élucidation. La biométrie, la technologie des empreintes génétiques individuelles, désormais à maturité, sont parmi les plus prometteuses. Mais bien d'autres existent, comme le traitement de la voix, des odeurs ou celui de l'image qui permettra de comparer des photos de signalisation à des portraits-robots ou à des séquences enregistrées par les moyens de vidéo-protection. Le développement des puces adn [3] sera aussi de nature à permettre l'exploitation, en temps réel, des traces biologiques.

La police technique et scientifique est un instrument d'une puissance importante en ce qu'il garantit, avec un taux d'erreur très faible lorsque les méthodes scientifiques sont respectées, la concordance entre deux profils, digitaux ou génétiques. Il s'agit donc d'un outil absolument indispensable à l'analyse des traces laissées sur les scènes de crime, surtout lorsqu'il n'existe aucun témoin. La faible part laissée à la subjectivité permet d'ailleurs aussi bien de confondre que de disculper une personne mise en cause.

La police technique et scientifique en général, particulièrement l'exploitation des traces laissées sur la scène du crime et leur comparaison avec celles enregistrées dans un fichier de police, a désormais pris une place très importante dans l'administration de la preuve pénale. En complément d'autres éléments, ces techniques permettent d'apporter aux enquêteurs des éléments de preuve objectifs et fiables. Par ailleurs, la preuve scientifique, qui était il y a encore très peu de temps réservée aux seuls crimes de sang, est désormais utilisée dans le traitement de la délinquance de masse.

Le fichier automatisé des empreintes digitales (faed) et le fichier national des empreintes génétiques (fnaeg), grâce à un investissement d'importance étalé sur plusieurs années, sont en voie de modernisation rapide. La législation leur assigne un statut particulier, étroitement contrôlé, d'une part dans l'alimentation, d'autre part dans les cas et les modalités de consultation.

La loi définit strictement le champ des personnes pouvant faire l'objet d'une signalisation. S'il peut être procédé à la comparaison ponctuelle d'empreintes

sur des témoins, il est nécessaire que des indices graves et concordants soient réunis pour qu'un profil individuel soit conservé dans le fichier.

Le mode de fonctionnement de ces fichiers repose sur la comparaison à un instant donné d'une empreinte anonyme relevée sur une scène d'infraction ou du profil d'un individu signalisé à l'occasion d'une enquête, avec l'ensemble des traces anonymes et des profils individuels figurant déjà dans la base. Il s'agit donc d'un rapprochement sur des données biométriques individuelles.

En raison de leur mode d'alimentation et de fonctionnement, ces fichiers sont exclusivement utilisés en police judiciaire, jamais dans un cadre de police administrative.

Le fichier des empreintes digitales fait l'objet, depuis début 2006, d'une alimentation automatisée et d'une consultation directe par l'enquêteur. Ce qui le rend désormais utilisable dans le délai de l'enquête de flagrance, voire de la garde à vue, quand il fallait auparavant plusieurs semaines pour sa consultation. Avec plus de 3,7 millions d'empreintes digitales enregistrées, le faed a permis de résoudre, en 2009, près de 10 000 affaires contre 7 000 en 2002. Le fichier des empreintes génétiques, avec 1,59 million de profils individuels et traces conservées, a permis le rapprochement de près de 45 800 rapprochements impliquant 108 698 profils dont près de 18 000 au cours de l'année 2010.

Le système de traitement des infractions constatées (stic) et le système judiciaire de documentation et l'exploitation (judex) sont constitués à partir de certaines informations extraites des procédures de police judiciaire établies par les enquêteurs. Leur finalité première est de faciliter la constatation des infractions pénales, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Ils permettent, par exemple, de repérer le caractère sériel ou répété de certains actes de délinquance, d'effectuer des rapprochements relatifs aux horaires, aux lieux, aux modes opératoires ou au profil des auteurs ou de leurs victimes. Ils sont tout particulièrement utiles pour la lutte contre les délinquants d'habitude. stic et judex demeurent à ce jour les premiers outils de résolution des enquêtes, avant même les fichiers d'empreintes digitales et génétiques. À l'occasion de leur refonte d'ensemble dans le logiciel de traitement des procédures judiciaires (tpj), qui devrait être déployé progressivement en 2012, leurs fonctionnalités de recherche judiciaire seront perfectionnées et leur mise à jour, sujet permanent de contestation légitime, accélérée et fiabilisée.

VI. Prévenir les menaces et anticiper les risques

La raison d'être d'un État est de protéger ses citoyens, de leur assurer la sécurité sur son territoire et en dehors de ses frontières. En pleine mondialisation, avec la libre circulation des individus, dans un monde troublé par des conflits faisant appel à des solidarités transnationales (religieuses, ethniques, culturelles), ce rôle est plus difficile à assumer qu'à l'époque où les individus restaient quasiment toute leur vie dans le périmètre de leur canton de naissance.

Dès lors, la protection n'est plus physique, mais immatérielle : c'est l'information. Une information pointue, qualitative, entretenue et vérifiée. C'est là le travail des services de renseignements, civil et militaire, qui doivent assurer notre sécurité intérieure et extérieure.

Anticipation et prévention sont les maîtres mots du renseignement opérationnel. Il ne s'agit pas ici de trouver les auteurs d'un crime ou d'un délit, mais de détecter, avant tout passage à l'acte, des individus dont le comportement, l'idéologie et les fréquentations laissent penser qu'ils pourraient chercher, en France ou à l'étranger, à mettre en péril nos intérêts stratégiques, à déstabiliser nos institutions et à frapper notre population ou ceux de nos alliés.

À cet effet, les services de renseignements disposent de fichiers – couverts par le secret – dans lesquels ils consignent de nombreuses informations concernant tous les individus potentiellement dangereux pour nos intérêts nationaux (espions, terroristes, militants politiques violents, nationalistes régionaux, etc.). Ces fichiers permettent de consolider la transmission de la mémoire opérationnelle entre les générations d'agents et sont un instrument de travail quotidien. Les services dédiés entretiennent également des relations étroites avec leurs homologues des pays alliés. Cette coopération permet d'améliorer sans cesse la connaissance des dangers qui sont évidemment protéiformes et très évolutifs.

La défense des intérêts nationaux et la raison d'État justifient ainsi l'existence de fichiers très sensibles qui échappent à tout contrôle judiciaire et en grande partie à celui de la cnil [4]. C'est donc au pouvoir exécutif seul, légitiment élu dans un cadre démocratique, de s'assurer qu'il n'y a aucune dérive dans la constitution et

l’utilisation de ces fichiers qui, d’une certaine façon, portent atteinte à certaines libertés individuelles, dans la mesure où ils imputent des intentions à des individus qui ne sont pas passés à l’acte, et dont on ne souhaite pas qu’ils passent à l’acte. Le groupe de contrôle des fichiers de police et de renseignement mis en place en 2006 et réactivé en 2008 a demandé qu’un dispositif adapté de contrôle soit mis en place pour sortir de cette exception.

Le renseignement opérationnel est donc une dimension essentielle, d’une part, de la prévention des menaces, d’autre part, de l’action de lutte contre la délinquance. En effet, l’ouverture d’un cadre d’enquête judiciaire suppose un minimum d’éléments convergents, si bien que certaines informations justifient des repérages ou recoupements complémentaires avant de pouvoir être exploitables dans le cadre d’une procédure judiciaire.

VII. Concourir aux enquêtes administratives

L’exercice de certaines professions ou l’accès à certains emplois sensibles nécessite de connaître le passé des postulants. En effet, l’État ou une entreprise ayant une activité dans un secteur sensible ne peut se permettre de confier certaines missions à des personnes qui ont commis des infractions graves ou qui font l’objet d’une surveillance de la part des services de renseignements.

L’article 17-1 de la loi n° 95-73 du 21 janvier 1995 d’orientation et de programmation relative à la sécurité autorise la consultation des fichiers, dits d’antécédents judiciaires, dans le cadre de la réalisation des enquêtes administratives.

L’article 25 de la loi n° 2003-239 du 18 mars 2003 relative à la sécurité intérieure a modifié cet article en élargissant les cas dans lesquels il peut être procédé à la consultation de ces fichiers de police judiciaire à des fins d’enquêtes administratives.

Aux termes de l’article 17-1 ainsi modifié, la consultation des fichiers de police judiciaire est autorisée dans le cadre d’enquêtes préalables aux décisions administratives de recrutement, d’affectation, d’agrément ou d’habilitation

concernant soit les emplois publics participant à l'exercice des missions de souveraineté de l'État, soit les emplois publics ou privés du domaine de la sécurité et de la défense.

La consultation des fichiers de police judiciaire est également prévue pour l'autorisation d'accès à des zones protégées en raison de l'activité qui s'y exerce et les autorisations concernant les matériels ou produits présentant un caractère dangereux (ex. : port d'armes).

Le décret n° 2005-1124 du 6 septembre 2005 (abrogeant le décret n° 2002-424 du 28 mars 2002, modifié par le décret n° 2005-307 du 24 mars 2005) précise la liste des emplois du secteur public et du secteur privé pouvant donner lieu à la consultation de ces fichiers de police judiciaire : agents de police municipale, agents de surveillance et de gardiennage, convoyeurs de fonds, membres des services d'ordre des organisateurs de manifestations sportives, récréatives ou culturelles. En 2005, plus de 120 000 enquêtes administratives ont été effectuées dans le cadre de la loi du 12 juillet 1983 sur la sécurité privée dont plus de 70 000 dans le seul domaine aéroportuaire.

L'article 17-1 de la loi précitée du 21 janvier 1995 prévoit en outre la consultation de ces fichiers pour « l'instruction des demandes d'acquisition de la nationalité française et de délivrance et de renouvellement des titres relatifs à l'entrée et au séjour des étrangers ainsi que pour la nomination et la promotion dans les ordres nationaux ».

Lors de l'examen, en octobre 2002, du projet de loi pour la sécurité intérieure, la cnil avait souligné que l'extension des cas de consultation des fichiers de police judiciaire à des fins administratives risquait de leur faire jouer : « Le rôle d'un casier judiciaire parallèle moins contrôlé, alors même que leur objet, leurs conditions d'accès, les modalités structurelles de leur alimentation et les délais inévitables de toute mesure d'effacement ou de mise à jour doivent en faire seulement un instrument de police judiciaire sauf dans quelques cas bien précis et rigoureusement contrôlés. »

Le Conseil constitutionnel dans sa décision sur la loi de sécurité intérieure (n° 2003-467 dc) en date du 18 mars 2003 a validé ce dispositif en déclarant « qu'aucune norme constitutionnelle ne s'oppose par principe à l'utilisation à des fins administratives de données nominatives recueillies dans le cadre d'activités de police judiciaire » et que ces consultations étaient assorties de garanties

suffisantes au regard du respect des libertés individuelles.

La loi et le règlement prévoient en effet différentes garanties pour la consultation des fichiers de police judiciaire dans le cadre d'enquêtes administratives.

L'article 6 du décret du 5 juillet 2001 modifié par le décret n° 2006-1258 du 14 octobre 2006 sur le stic prévoit à cet égard une limitation des informations accessibles.

Ainsi, les consultations effectuées dans le cadre d'enquêtes administratives ne permettent pas d'accéder aux informations relatives aux victimes ni à celles concernant les personnes mises en cause ayant bénéficié d'une suite judiciaire favorable (non-lieu et classement sans suite motivés par une insuffisance de charges).

Cependant, contrairement à l'article 6 du décret du 5 juillet 2001 originel qui limitait la consultation à des fins administratives (dans des cas exceptionnels) aux seules informations qui se rapportaient à des procédures judiciairement closes, l'article 25 de la loi du 18 mars 2003 étend cette possibilité de consultation aux données portant sur des procédures judiciaires en cours.

C'est essentiellement à l'occasion de la consultation des fichiers stic et judex en police administrative, et des difficultés qu'elle peut révéler, que le débat public sur les fichiers de police s'est focalisé. Ces consultations sont de pratique ancienne, mais ont fait l'objet d'un encadrement et d'une normalisation au cours de la dernière décennie, surtout lorsque l'agrément préfectoral préalable à l'accès à certaines professions réglementaires a été renforcé pour des motifs de moralisation et de prévention de certains risques.

Il convient en outre de dissocier clairement l'inscription dans le stic ou le judex et la décision administrative qui est prise après leur consultation. La décision préfectorale d'agrément ne doit pas être mécaniquement liée par l'inscription dans un fichier de police consultable en police administrative. En aucun cas, la seule mention dans l'un de ces fichiers ne justifie automatiquement une décision de refus.

Il convient de rappeler que doivent seuls être enregistrés dans ces fichiers des faits considérés comme avérés par les officiers de police judiciaire – à savoir, étayés par des indices graves et concordants. Les données relatives aux témoins

ne sont jamais enregistrées et celles relatives aux victimes ne sont pas consultables en police administrative.

Le préfet est tenu de prendre en compte la gravité, l'ancienneté, l'éventuelle répétition des faits et, naturellement, le lien qui existe entre les faits commis antérieurement et les garanties requises pour la décision administrative en cause. Le préfet dispose donc de la marge de manœuvre suffisante pour apprécier certaines situations personnelles et a même le devoir, à peine d'annulation, d'exercer un jugement de proportionnalité.

L'absence à ce jour de système d'information automatisé cohérent sur l'ensemble de la chaîne pénale pose cependant des difficultés importantes pour la mise à jour de ces fichiers à partir des décisions de justice relatives aux affaires ayant donné lieu à inscription, lorsque celles-ci sont plus favorables au mis en cause que la procédure établie par l'officier de police judiciaire. Ce point devrait être résolu au cours des prochaines années, ce qui illustre concrètement l'intérêt, y compris pour les droits des personnes, que peut représenter une interconnexion encadrée et limitée de certains fichiers de la chaîne pénale.

Notes

[1] Système d'identification des individus inventé par Alphonse Bertillon à partir de données anthropométriques.
[2] Le traitement du renseignement. L'informatisation du fichier central*Tribune du commissaire de police*, juin 1985
[3] Les puces à adn permettent de visualiser et de mesurer très rapidement des différences d'expression entre les gènes pour le génome complet d'un organisme. C'est ainsi que sur une seule puce, l'ensemble du génome humain (~ 33 000 gènes) peut être analysé en une seule étape.
[4] Les fichiers classés « secret défense » sont soumis aux contrôles exercés par la cnil, dossier par dossier, à l'occasion du droit d'accès indirect.

Chapitre II

État des lieux

La France, comme la plupart des États modernes, compte de nombreux traitements automatisés de données à caractère personnel tenus par l'Administration ou des organismes publics et parapublics. Ils ont pour objectif de faciliter le travail des agents et des services de l'État et couvrent de très nombreux secteurs d'activité de l'Administration française : sécurité intérieure, défense nationale, recensement des personnes de nationalité française et étrangère ou des contribuables, gestion des assurés sociaux, des personnes sans emploi, des allocataires du rmi ou de prestations familiales, comptabilisation du nombre de véhicules en circulation ou de titulaires de permis de conduire, enregistrement des décisions de justice ou encore gestion des détenus et des prévenus, etc.

Par négligence ou habitude, certains fichiers n'ont pas été déclarés. Ils sont le plus souvent irréguliers. Leur déclaration n'aurait pas posé de problèmes majeurs, mais elle n'a pas été réalisée (les fichiers des fourrières, par exemple [1]). D'autres sont en avance sur la loi et ont été expérimentés hors cadre légal (les fichiers d'analyse sérielle [2]), ce qui ne réduit par leur irrégularité, mais dépasse le simple oubli. Un petit nombre est parfaitement illégal, portant sur des recensements interdits par la loi, et n'a pas vocation à évoluer. Seule leur destruction est alors acceptable.

I. Les applications bureautiques

Comme toute structure organisée, hiérarchisée et moderne, la Police et la Gendarmerie nationales exercent leurs missions en ayant recours à des systèmes de gestion bureautiques informatisés. Ceux-ci ne sont pas au sens légal et utilitaire des traitements automatisés de données à caractère nominatif. Ils participent de l'efficacité et de la rapidité de la réponse des forces de l'ordre tout

en contribuant au suivi indispensable des patrouilles, des agents et des événements gérés par ces deux institutions.

1. Les applications de la Gendarmerie nationale

La Gendarmerie nationale s'appuie principalement sur les systèmes aramis, puls@r et lrpgn.

L'application aramis est un système de traitement des informations présentant un caractère opérationnel. Elle a pour objet d'informer les autorités hiérarchiques des événements en cours, de leur évolution et de leurs développements. aramis contient certaines données nominatives (nom, prénom, domiciliation, téléphone) qui sont enregistrées lorsqu'une personne signale un fait à l'opérateur du Centre opérationnel et de renseignement de la Gendarmerie (corg). Les informations nominatives sont effacées au bout de trois mois. Ce système sera prochainement remplacé par le système d'information bases de données de sécurité publique (bdsp) qui conduira progressivement à la disparition d'aramis (voir *supra*).

En 2011, le traitement puls@r, évolution de l'application Bureautique Brigade 2000, a été déployé dans les brigades de Gendarmerie. Cette application permet aux unités territoriales de la Gendarmerie nationale de gérer, sur le plan administratif, le service et les registres (courriers et procès-verbaux), les amendes forfaitaires, ainsi que de générer les messages d'information statistique relatifs à la délinquance et les bulletins d'analyse des accidents relatifs à l'accidentalité. Quatre modules ont été créés par arrêté : 1) gestion des amendes forfaitaires et des consignations dénommé « gestion des amendes forfaitaires des unités » élémentaires de la gendarmerie départementale et des gendarmeries spécialisées ; 2) gestion des messages d'information statistique et des bulletins d'analyse des accidents des unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées, dénommé « gestion des mis et des baa » ; 3) gestion des courriers et des procédures dans les unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées, dénommé « gestion du registre des unités » ; 4) gestion du service dans les unités élémentaires de la gendarmerie départementale et des gendarmeries spécialisées, dénommé « gestion du service des unités ».

Le logiciel « Logiciel de rédaction des procédures de la Gendarmerie nationale » (lrpgn – ex-Ic@re) est destiné à assister les militaires de la Gendarmerie dans la rédaction de leurs procès-verbaux. Cet outil participe, par ailleurs, à la remontée d'informations en alimentant les bases de données opérationnelles (Judex puis, lorsqu'il sera mis en service, tpj). lrpgn a été autorisé par le décret n° 2011-111 du 27 janvier 2011.

2. Les outils de la Police nationale

La Police nationale devrait utiliser, en 2011, le « Logiciel de rédaction des procédures de la Police nationale, V2 » (ex-ardoise) destiné à uniformiser la rédaction de procédures et à alimenter notamment le futur fichier traitement des procédures judiciaires (tpj – ex-ariane), qui remplacera à la fois le stic de la Police nationale et le judex de la Gendarmerie nationale. Plus qu'un simple logiciel d'assistance à la rédaction des procédures, lrppn est le cœur du nouveau système d'information de la police nationale. lrppn V2 constituera donc, dans sa version définitive qui interviendra au terme des améliorations techniques successives (lrppn 3), un support technique unique de l'activité procédurale de l'ensemble des services de la Police nationale dans l'exercice de leurs missions de police judiciaire et administrative et l'outil d'alimentation des traitements nationaux de documentation criminelle (traitement des procédures judiciaires, fichiers des objets et véhicules signalés). lrppn V2 permet la collecte et l'archivage des informations recueillies par les services chargés de l'établissement des procédures diligentées dans le cadre de leurs missions de police judiciaire ou administrative. Les données enregistrées sont donc issues des procès-verbaux, comptes rendus d'enquêtes et rapports administratifs ou judiciaires. Il faudra toutefois attendre la version 3 pour que le lrppn puisse alimenter d'autres traitements dont tpj, le système du ministère de la Justice Cassiopée ou le module statistiques (état 4001 et statistiques opérationnelles). Après une expérimentation de plusieurs mois en 2010, le décret autorisant le déploiement de lrppn V2 a été publié le 29 janvier 2011 *(décret n° 2011-110)*. La version 3 devra faire l'objet d'une nouvelle autorisation. Elle serait déployée fin 2011/début 2012.

Pour la gestion des effectifs, des interventions et événements et des patrouilles, mais également pour l'enregistrement des signalements d'usagers, la Police nationale emploie, depuis 1995, *la main courante* qui a été généralisée et

informatisée (mci) depuis le 1er janvier 2005, dans l'ensemble des circonscriptions de sécurité publique. La mci permet de suivre en permanence l'activité d'un service. Les statistiques établies à partir des données de la mci permettent de mesurer avec précision les contraintes et les marges de manœuvre, ainsi que l'adéquation entre la répartition temporelle des phénomènes d'insécurité et la distribution horaire des effectifs. Enfin, les comptes rendus d'intervention et les déclarations du public constituent une source d'informations pour les enquêteurs. En effet, ces données peuvent aider à caractériser des situations délictuelles (occupation de hall d'immeuble, trafic de stupéfiants, etc.) ou à élucider des affaires judiciaires (recherche de domiciles, de fréquentations ou de véhicules). Une nouvelle version devrait être mise en œuvre en 2011/2012 (le projet de décret a été transmis à la cnil le 5 novembre 2010).

3. Le traitement automatisé du service central de préservation des prélèvements biologiques (scppb)

Un autre système peut être considéré comme une application bureautique : le traitement automatisé du service central de préservation des prélèvements biologiques (scppb) qui a pour finalité d'assurer la gestion des prélèvements biologiques recueillis sur une scène de crime ou de délit pour l'une des infractions mentionnées à l'article 706-55 du Code de procédure pénale à l'occasion des procédures de recherche des causes de la mort : (cadavres non identifiés) ou lors des procédures de recherche des causes d'une disparition (personnes disparues).

II. Les fichiers administratifs

Certains fichiers sont dits « techniquement neutres » car ils regroupent des informations objectives sur des personnes ou des objets. Ce sont des fichiers qui se contentent d'enregistrer des données administratives sur des personnes, objets ou moyens de transport.

1. Le fichier de la batellerie

Créé en 1942 afin d'assurer le suivi des mariniers ainsi que celui des bateaux affectés au transport fluvial de marchandises et des compagnies fluviales, et géré par la Gendarmerie nationale, il a été détruit en 2010 conformément aux dispositions de la loi de 2004.

2. Le fichier des personnes nées à l'étranger (fpne)

Créé en 1975 pour la Gendarmerie nationale, il s'agit d'un fichier mécanographique. À l'instar du fichier alphabétique de renseignements (far), il est constitué de sept millions de fiches cartonnées individuelles. Il a pour objet de collationner les renseignements relatifs aux personnes nées hors de France. Le fpne est actuellement stocké à l'état d'archive et ne fait plus l'objet de consultations ni d'une administration fonctionnelle.

3. Le fichier des passagers aériens (fpa)

Il a pour but d'améliorer le contrôle aux frontières, de lutter contre l'immigration clandestine et de contribuer à la prévention et à la répression des actes de terrorisme. Il a été rendu nécessaire suite à la directive du 29 avril 2004 du Conseil de l'Union européenne instituant l'obligation, pour les transporteurs, de communiquer des données personnelles relatives à leurs passagers et introduite dans le droit interne par l'article 7 de la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. Le traitement est interconnecté avec le fichier des personnes recherchées (fpr) et le système d'information Schengen (sis). La durée de conservation des données est de cinq ans pour la lutte contre le terrorisme et vingt-quatre heures pour la lutte contre l'immigration clandestine. Une procédure automatique de suppression des données est mise en œuvre. Au 4 février 2010, 359 961 passagers ont été enregistrés dans la base de données (depuis le 1er mai 2007). L'expérimentation, prévue par l'arrêté du 28 janvier 2009 pour une durée deux ans, a été prolongée jusqu'au 31 décembre 2011.

4. L'application de gestion du répertoire informatisé des propriétaires et possesseurs

d’armes (agrippa)

Il s’agit d’un traitement automatisé de données à caractère personnel concernant la gestion et le suivi des détentions d’armes et de munitions. Il a pour finalité l’enregistrement et le suivi des autorisations et des récépissés de déclarations délivrés par l’autorité administrative relatifs au régime des matériels de guerre, armes et munitions des 1re et 4e catégories [3] et des armes et éléments d’armes soumis à déclaration des 5e et 7e catégories.

5. Le fichier national des interdictions de stade (fnis)

Dans le cadre de la politique de prévention et de lutte contre les violences lors des manifestations sportives, ce fichier a été créé en août 2008. Il a notamment pour finalité de garantir la pleine exécution des mesures d’interdictions administratives et judiciaires de stade, en facilitant les contrôles aux abords et dans les enceintes sportives, le suivi et la surveillance des supporteurs à risque ayant déjà fait l’objet d’une mesure d’interdiction, en permettant à l’autorité préfectorale, le cas échéant, de mieux apprécier le comportement d’ensemble adopté par les intéressés à l’occasion de différentes manifestations sportives et en réalisant des statistiques.

6. Le fichier national transfrontière (fnt)

Créé en 1991, il a été modifié par la loi du 23 janvier 2006 relative à la lutte contre le terrorisme. Exploité par la direction centrale de la police aux frontières, le fnt a pour finalité d’assurer l’amélioration du contrôle aux frontières et la lutte contre l’immigration clandestine ainsi que la prévention et la répression des actes de terrorisme.

III. Les fichiers à vocation judiciaire

Dans le cadre de leurs missions de police judiciaire, la Police et la Gendarmerie

nationales gèrent des fichiers de travail qui seront utilisés lors des enquêtes judiciaires.

1. Le fichier des brigades spécialisées (fbs)

La direction centrale de la Police judiciaire emploie le fichier des brigades spécialisées (fbs) créé en 1991 pour les services de police spécialisés luttant contre la grande délinquance et le crime organisé (banditisme, terrorisme, stupéfiants, proxénétisme, trafics d'œuvres d'art, de fausse monnaie, blanchiment, grande délinquance financière, immigration clandestine). L'objectif du fbs est de collecter des informations sur l'environnement et les habitudes des délinquants spécialisés et de favoriser la coopération des services. Il comportait 206 999 fiches au 31 décembre 2009. Le fbs devrait faire l'objet d'une future modernisation.

2. Le fichier de travail de la police judiciaire (ftpj)

La même direction utilise également le fichier de travail de la police judiciaire (ftpj), conçu en 1987. Le contenu du fichier de travail est identique à celui du fichier des brigades spécialisées (fbs) mais, contrairement à ce dernier qui permet un échange d'informations entre services spécialisés, le ftpj n'est constitué que de bases locales au sein des services régionaux de police judiciaire, non connectées entre elles. Ce fichier n'est plus actuellement utilisé que par quelques services territoriaux de police judiciaire.

3. Le fichier du faux monnayage (fnfm)

Il a été créé pour satisfaire aux obligations européennes définies par le règlement européen n° 1338/2001 du 28 juin 2001 relatif à la protection de l'euro contre le faux monnayage. Il recense l'ensemble des affaires de fausse monnaie commises sur le territoire national et sert de base de données de documentation et d'analyse opérationnelle. Ce fichier sert également à l'alimentation du système d'information d'Europol. Il permet aussi la gestion des statistiques sur les saisies « police » et « gendarmerie » pour les contrefaçons de l'euro, les devises et les

officines de fausse monnaie découvertes sur le territoire national.

4. Le fichier des véhicules et des objets volés (fvv et fos)

Autorisé par un arrêté du 15 mai 1996 (modifié en 2005), le *fichier des véhicules volés* (fvv) est utilisé quotidiennement par les forces de police et de gendarmerie. Il répertorie au plan national les véhicules, bateaux et aéronefs signalés volés ou détournés par leur propriétaire ou mis sous surveillance à la demande d'un service de police ou de gendarmerie. Le fvv indique également aux policiers, aux gendarmes et aux douaniers la conduite à tenir en cas de découverte. Au 1er novembre 2010, le fvv regroupait 420 280 fiches. Il devrait faire l'objet d'un arrêté modificatif rendant destinataires des informations les agents de police municipale.

Le *fichier des objets signalés* (fos) constitue un fichier dit de contrôle en présence. Il permet de connaître si un objet bien identifié (par un numéro de manufacture ou l'identité de son propriétaire) a été signalé par les unités de gendarmerie à l'occasion d'une enquête judiciaire ou par le système d'information Schengen (sis) comme étant volé.

En 2011/2012, le fvv et le fos seront remplacés par un nouveau fichier : le fichier des objets et véhicules signalés (foves) regroupant les véhicules et les objets volés signalés par les services de police et les unités de la gendarmerie.

IV. Les fichiers de renseignement

Les fichiers de renseignement sont généralement ceux qui soulèvent le plus de questions et entretiennent les inquiétudes de l'opinion publique. Ils ne concentrent pas nécessairement des informations sur des personnes qui ont déjà eu affaire aux services répressifs, mais sur celles qui sont susceptibles de commettre des crimes ou des délits et qui doivent, au regard de certains éléments, faire l'objet d'une surveillance plus soutenue des forces de l'ordre. Ce sont des bases de données liées aux missions de renseignement de la Police et de la Gendarmerie nationale. Les éléments « qualitatifs » prédominent dans ces fichiers qui ont pour principale finalité d'aider les forces de l'ordre à prévenir la

criminalité et les actes de terrorisme. Certains d'entre eux sont couverts par le secret défense et bénéficient du régime dérogatoire ouvert par les articles 30 (I) et 44 (IV) de la loi de 1978 (non-publication de l'acte de création et absence de droit de contrôle sur place de la cnil). Des propositions ont été émises par le groupe de contrôle des fichiers de police et de gendarmerie pour mettre fin à cette exception.

1. 1. Le fichier alphabétique du renseignement (far)

Se présentant sous forme de fiches manuscrites individuelles gérées localement, les fichiers alphabétiques de renseignements (far) avaient pour vocation de permettre aux militaires des unités opérationnelles de la Gendarmerie nationale d'acquérir une connaissance approfondie de leur population résidente, en particulier sur leur « dangerosité ». L'obsolescence du far, liée principalement à sa gestion très lourde, ainsi que les contraintes légales relatives au respect des libertés individuelles, a entraîné la destruction du far en 2010. Seules ont été conservées, pour les archives, les fiches de quatre brigades territoriales.

2. cristina

La réorganisation des services de renseignement du ministère de l'Intérieur, intervenue le 1er juillet 2008, a entraîné la création d'un service de renseignement intérieur civil unique [4], chargé des missions de l'ancienne direction de la Surveillance du territoire et d'une partie de celles de l'ancienne direction centrale des Renseignements généraux. Un nouveau fichier a donc dû être créé pour la direction centrale du Renseignement intérieur (dcri) : Centralisation du renseignement intérieur pour la sécurité du territoire et les intérêts nationaux (cristina). Ce traitement, comme le fichier de la dst (qui datait de 1986), est soumis au régime juridique des fichiers « de souveraineté », défini par l'article 26 (III) de la loi du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés et par le décret n° 2007-914 du 15 mai 2007. cristina ne peut faire l'objet d'un contrôle sur place de la cnil et le décret en portant création n'est pas publié. Les données ne sont enregistrées et conservées qu'en fonction des finalités (très strictement délimitées) du fichier et donc, pour l'essentiel, de

l’intérêt qu’elles présentent au regard de la sûreté de l’État et de la sécurité nationale.

3. Gesterex

La mise en œuvre de la réforme du renseignement intérieur au sein de la préfecture de Police a entraîné la création d’une direction du Renseignement de la préfecture de Police (dr-pp). La dr-pp concourt à l’activité de la dcri pour la prévention des actes de terrorisme et pour la surveillance des individus, groupes, organisations et phénomènes de société susceptibles, par leur caractère radical, leur inspiration ou leurs modes d’action, de porter atteinte à la sécurité nationale. À ce titre, elle dispose du fichier Gestion du terrorisme et des extrémismes à potentialité violente (gesterex). Ce traitement, comme le fichier cristina, est soumis au régime juridique des fichiers « de souveraineté », défini par l’article 26 (III) de la loi du 6 janvier 1978 relative à l’informatique, aux fichiers et aux libertés.

4. Prévention des atteintes à la sécurité publique (pasp)

L’application concernant la prévention des atteintes à la sécurité publique fait suite aux mêmes nécessités issues de la réforme des services de renseignement. Une partie des missions qui étaient dévolues aux renseignements généraux a été basculée vers la sécurité publique et vers le nouveau service de l’information générale. Il s’agit notamment des missions de renseignement liées aux violences urbaines, aux dérives sectaires, au radicalisme religieux ou encore à l’information générale du Gouvernement. Un nouveau fichier, reprenant une très grande partie des informations contenues dans l’ancien fichier des renseignements généraux sorti de la clandestinité en 1991, a donc dû être mis en place. Faisant suite à une première version – edvige – qui avait suscité la polémique en septembre 2008, puis au projet edvirsp, le fichier pasp est destiné à recueillir, conserver et analyser les informations qui concernent des personnes dont l’activité individuelle ou collective indique qu’elles peuvent porter atteinte à la sécurité publique, notamment les informations qui concernent les personnes susceptibles d’être impliquées dans des actions de violences collectives, en particulier en milieu urbain ou à l’occasion de manifestations sportives.

Contrairement à son prédécesseur, ce traitement supprime la possibilité de centraliser les informations relatives à des personnes exerçant un mandat ou jouant un rôle institutionnel, économique, social ou religieux significatif. Ce fichier est aussi désormais distinct de celui relatif aux enquêtes administratives (voir *supra*).

Le groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie a toutefois souhaité la suppression de la mention « origines géographiques » qui pourrait porter à confusion [5].

5. Gestion des violences urbaines (gevi)

Conçu en 1996 par la préfecture de police de Paris, cette application a pour base juridique le décret n° 921-1051 du 14 octobre 1991. gevi constitue un traitement comprenant des données sur des individus majeurs ou des personnes morales susceptibles d'être impliqués dans des actions de violences urbaines ou de violences sur les terrains de sport. Son exploitation permet d'effectuer des rapprochements et d'établir des liens entre des individus, des groupes, des événements et des faits. Aucune durée de conversation n'est actuellement prévue. Il est envisagé que gevi soit étendu à l'ensemble du territoire national et permette l'enregistrement des mineurs dans le cadre du cadre juridique de pasp.

6. Enquêtes administratives liées à la sécurité publique (easp)

Le fichier utilisé pour les personnes faisant l'objet d'enquêtes administratives visant à déterminer si leur comportement n'est pas incompatible avec l'exercice des fonctions ou des missions envisagées compte tenu de leur nature (en application des dispositions du premier alinéa de l'article 17-1 de la loi du 21 janvier 1995), est désormais distinct du fichier pasp (et donc de l'ex-fichier des renseignements généraux) et a été créé par le décret n° 2009-1250 du 16 octobre 2009 : enquêtes administratives liées à la sécurité publique (easp). Il devrait être complété par un nouveau décret permettant aussi la réalisation, par les fonctionnaires de police chargés du renseignement, des enquêtes administratives en vue de l'instruction de dossiers de demande d'acquisition de la nationalité française et des demandes de titres de séjour. Les données peuvent être

conservées pendant une durée maximale de cinq ans à compter de leur enregistrement. Les données ne peuvent concerner des mineurs que s'ils sont âgés de 16 ans au moins et ont fait l'objet d'une enquête administrative. Les consultations du traitement automatisé font l'objet d'un enregistrement comprenant l'identifiant du consultant, la date, l'heure et l'objet de la consultation.

7. Le fichier des courses et jeux

Créé par arrêté du 8 novembre 2010, ce traitement est l'héritier du traitement qui était géré par le service « Courses et jeux » de la direction centrale des Renseignements généraux, disparu et transféré à la direction centrale de la Police judiciaire, à la suite de la réforme des services de renseignement en 2010. Il a pour finalité d'assurer la surveillance de la régularité et de la sincérité des jeux, des courses et des paris, par la conservation des données recueillies, notamment à l'occasion des enquêtes administratives d'agrément et d'autorisation de jeux, ou relatives aux personnes faisant l'objet d'une mesure d'interdiction ou d'exclusion des salles de jeu ou des champs de courses.

V. Les fichiers d'antécédents judiciaires

Les fichiers d'antécédents judiciaires forment une autre catégorie de fichiers indispensable à l'action policière puisqu'ils constituent la mémoire judiciaire de l'activité de police. Il s'agit principalement aujourd'hui du système de traitement des infractions constatées (stic) et du système judiciaire de documentation et d'exploitation (judex) respectivement mis en œuvre par les services de police et par les unités de gendarmerie, qui font actuellement l'objet d'une modernisation dans le cadre du projet Traitement des procédures judiciaires (tpj).

Ces fichiers collectent certaines informations extraites des procédures de police judiciaire réalisées par les enquêteurs. Leur finalité première est de faciliter la constatation des infractions pénales, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs. Ils permettent notamment mais de façon très limitative d'effectuer des rapprochements entre différentes affaires

présentant des similitudes mais surtout de matérialiser, dès la phase d'enquête, l'état de récidive de certains auteurs de crimes ou délits.

stic et judex, s'ils sont également utilisés dans des conditions et dans le cadre d'enquêtes administratives strictement autorisées par la loi [6], demeurent à ce jour les principaux outils d'orientation des enquêtes, alors que les fichiers d'empreintes digitales et génétiques sont aujourd'hui les principaux outils permettant l'identification formelle des auteurs.

La loi d'orientation et de programmation de la performance de la sécurité intérieure (lopssi), adoptée le 8 février 2011, a prévu plusieurs chapitres consacrés aux fichiers de police et de gendarmerie, dont un sur les fichiers d'antécédents. L'article 11 de la loi (art. 230-6 nouveau du Code de procédure pénale) pose ainsi le principe général autorisant les fichiers d'antécédents : « Afin de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions et la recherche de leurs auteurs, les services de la Police nationale et de la Gendarmerie nationale peuvent mettre en œuvre des traitements automatisés de données à caractère personnel recueillies :

1. au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire et concernant tout crime ou délit ainsi que les contraventions de la cinquième classe sanctionnant : *a)* un trouble à la sécurité ou à la tranquillité publiques, *b)* une atteinte aux personnes, aux biens ou à l'autorité de l'État ;

2. au cours des procédures de recherche des causes de la mort mentionnées à l'article 74 ou de recherche des causes d'une disparition mentionnées à l'article 74-1. Ces traitements ont également pour objet l'exploitation des informations recueillies à des fins de recherches statistiques. »

Ces traitements peuvent contenir des informations sur les personnes, sans limitation d'âge, à l'encontre desquelles il existe des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer, comme auteurs ou complices, à la commission des infractions prévues au texte. De même, les victimes peuvent y être enregistrées. Placé sous le contrôle du procureur de la République territorialement compétent, un magistrat, désigné par le ministre de la Justice, est spécialement chargé de suivre la mise en œuvre et la mise à jour de ces fichiers.

1. Le système d’information judiciaire de la Gendarmerie nationale (judex)

judex (acronyme pour système JUdiciaire de Documentation et d’EXploitation) met à la fois en œuvre des moyens centraux de traitement automatisé, qui recouvrent les applications judex-Affaires et judex-Personnes mises en cause, et des moyens déconcentrés au niveau de chaque département (décret n° 2006-1411 du 17 novembre 2006. Circulaire n° 51992 def/gend/oe/sdpj/pj du 10 août 2007). judex fournit aux enquêteurs de la Gendarmerie, de la Police nationales et de la douane judiciaire, une aide à l’enquête judiciaire (recherche sur les personnes et les objets, rapprochements entre auteurs et manière(s) d’opérer, identification des délinquants et des personnes disparues, recherche des antécédents d’une personne ayant fait l’objet d’une procédure, etc.). Le fichier est constitué de données recueillies dans les procédures établies par les unités de la Gendarmerie nationale ou par des services de la Police nationale et des agents des douanes habilités à exercer des missions de police judiciaire. Ces données concernent des personnes à l’encontre desquelles sont réunis, lors de l’enquête préliminaire de l’enquête de flagrance ou sur commission rogatoire, des indices graves ou concordants rendant vraisemblable qu’elles aient pu participer, comme auteurs ou complices, à la commission d’un crime, d’un délit ou de certaines contraventions de 5e classe, ou les victimes de ces infractions. En décembre 2008, judex rassemblait 9 811 933 fiches « affaires » et 2 145 329 personnes mises en cause.

2. Le système de traitement des infractions constatées (stic)

Autorisé par le décret n° 2001-583 du 5 juillet 2001 (modifié par le décret n° 2006-1258 du 14 octobre 2006), le système de traitement des infractions constatées (stic) est le fichier d’antécédents judiciaires de la Police nationale. Il permet l’exploitation des informations provenant des comptes rendus d’enquêtes issus des procédures pénales, à des fins de recherches criminelles et statistiques. Il s’agit d’un outil d’aide à l’enquête qui offre une information sur la criminalité et facilite la gestion de la documentation en répertoriant les références d’archivage des procédures.

Le stic peut également être consulté sous conditions dans le cadre des enquêtes administratives. Comme pour judex, les données enregistrées portent sur les mis en cause pour crimes, délits et certaines contraventions de 5e classe. Les informations contenues dans le stic ne sont que des extraits du contenu des procédures judiciaires (lesquelles font l'objet d'un archivage séparé). Les personnes qui peuvent faire l'objet d'un enregistrement sont celles à l'encontre desquelles sont réunis des indices graves ou concordants rendant vraisemblable qu'elles aient pu participer à la commission de l'infraction, lors de l'enquête préliminaire, de flagrance ou sur commission rogatoire, ou les victimes de ces infractions. D'autres informations peuvent être collectées : informations non nominatives qui concernent les faits objets de l'enquête, les lieux, dates de l'infraction et modes opératoires ; informations relatives aux objets. Les données peuvent être conservées, pour les majeurs, vingt ans en principe (mais cinq ans pour les infractions les moins graves, quarante ans pour certains délits graves énumérés dans le décret) ; pour les mineurs, cinq ans en principe (mais dix ou vingt ans pour certaines infractions graves) et pour les victimes, jusqu'à quinze ans (sauf opposition de la victime dans les cas prévus par la loi). La base nationale du stic contenait au 1er décembre 2010 les antécédents de 6,2 millions d'individus mis en cause, plus de 41 millions de dossiers de procédures (représentant 46 millions d'infractions), 37,9 millions d'enregistrements de victimes et 11 millions d'objets inscrits dans la base « objets ». Au 1er janvier 2010, 97 944 personnes étaient habilitées à consulter le stic. Il a fait l'objet de plus de six millions de consultations au 1er semestre 2010.

Ces deux fichiers doivent être remplacés à la fin 2011 par l'application Traitement des procédures judiciaires commune à la Police et à la Gendarmerie nationales.

Le stic-canonge : créé en 1950 par l'inspecteur principal René Canonge de la sûreté urbaine de Marseille (fichier signalétique manuel avec photographie), le fichier dit « Canonge » a été informatisé en juin 1992. Ce fichier permet de rassembler dans un même fonds documentaire le signalement des auteurs d'infractions à l'échelon d'une circonscription, d'un département, du ressort territorial d'un srpj ou d'une dipj, du service central de documentation criminelle. Il permet de rechercher des auteurs déjà connus des services de police à partir d'éléments de signalements fournis par le témoin ou la victime. Dans la partie signalement, ce fichier contient notamment un filtre sur le « type » composé de 12 catégories : blanc (Caucasien), méditerranéen, gitan, moyen-

oriental, nord-africain maghrébin, asiatique eurasien, amérindien, indien (Inde), métis-mulâtre, noir, polynésien, mélanésien-canaque.

Lors de ses travaux, en 2008, le groupe de contrôle sur les fichiers de police et de gendarmerie avait débattu de la possibilité de supprimer la classification ethnique pour aller vers un dispositif d'identification selon une grille chromatique (proposition soutenue notamment par les avocats et le secteur associatif). Cette évolution avait notamment pour objectif de limiter les présupposés physiques et de s'adapter à une société de plus en plus diverse et métissée. Cette proposition n'a pas fait l'unanimité et n'a donc pas été retenue. Seule la suppression du type « gitan » a été actée.

Dans sa réponse aux recommandations du groupe de contrôle, la ministre de l'Intérieur, de l'Outre-mer et des Collectivités territoriales a proposé de faire étudier le procédé du portrait-robot informatisé dans le cadre d'une première expérimentation départementale.

VI. Les fichiers d'identification judiciaire

Les fichiers d'identification judiciaire sont sûrement les fichiers les plus connus. Ils ont récemment fait l'objet d'une modernisation et d'un développement accéléré au regard de l'évolution de la science et des techniques. Depuis la fin du xixe siècle, qui a vu l'adoption des empreintes digitales comme outil de l'enquête criminelle, la science a fait d'énormes progrès, qui se traduisent par de nouveaux outils d'aide à l'identification des personnes et à l'élucidation. En raison de leur mode d'alimentation et de fonctionnement, ces fichiers sont exclusivement utilisés en police judiciaire, jamais dans un cadre de police administrative.

1. Le fichier judiciaire national automatisé des auteurs d'infractions sexuelles (fijais)

Le fijais, créé par la loi du 9 mars 2004, est entré en service le 30 juin 2005. Le

ministère de la Justice est responsable et gestionnaire du fijais. Il est tenu par le service du casier judiciaire national (cjn) et est placé sous le contrôle du magistrat qui le dirige. Le fijais a pour objectif de prévenir la récidive des auteurs d'infractions sexuelles ou violentes et de faciliter l'identification des auteurs de ces infractions.

Sont inscrites au fijais non seulement les personnes condamnées, même non définitivement, pour une des infractions suivantes : meurtre ou assassinat d'un mineur précédé ou accompagné d'un viol, de tortures ou d'actes de barbarie, agression ou atteinte sexuelle ou proxénétisme à l'égard d'un mineur, recours à la prostitution d'un mineur prévues par les articles 222-23 à 222-31, 225-7 (1o), 225-7-1, 225-12-1, 225-12-2 et 227.22 à 227-27 du Code pénal, meurtre ou assassinat commis avec tortures ou actes de barbarie, tortures ou actes de barbarie, meurtres ou assassinats commis en état de récidive légale, mais également, concernant ces mêmes infractions, les personnes ayant exécuté une composition pénale, été mises en examen par une juridiction d'instruction, ayant fait l'objet d'un non-lieu, d'une relaxe ou d'un acquittement fondé sur des motifs tenant à l'abolition des facultés de discernement (art. 122-1 du Code pénal) ou encore, s'agissant de ressortissants français, ayant été condamnées à l'étranger pour une de ces infractions. Les informations sont conservées pendant vingt ou trente ans selon la gravité de l'infraction commise. Ont accès au fichier les autorités judiciaires, la police et la gendarmerie, les préfets et les administrations de l'État qui sont définies par décret. Le ministère de l'Intérieur est alerté par le gestionnaire du fijais : des nouvelles inscriptions, des modifications d'adresse de personnes déjà inscrites et de l'identité des personnes qui n'ont pas justifié de leur adresse dans les délais prévus. Tout accès au fijais est tracé et archivé durant trois ans.

2. Le fichier automatisé des empreintes digitales (faed)

Créé par le décret nº 87-249 du 8 avril 1987 (modifié en 2005), le fichier automatisé des empreintes digitales (faed) est un fichier commun à la Police et à la Gendarmerie nationales. Il permet d'identifier les traces digitales et palmaires relevées sur les scènes d'infraction afin de rechercher et d'identifier les auteurs de crimes ou de délits ainsi que de détecter les usurpations d'identité et les identités multiples. Il est placé sous le contrôle d'un magistrat de l'ordre

judiciaire.

Le faed contient :

- les traces relevées au cours des enquêtes judiciaires ou sur ordre de recherches délivré par une autorité judiciaire ;
- les traces relevées à l'occasion d'une enquête ou instruction pour recherche des causes d'une disparition inquiétante ou suspecte (art. 74-1 et 80-4 du cpp) ;
- les empreintes relevées, dans le cadre des enquêtes pour crimes ou délits, sur les personnes à l'encontre desquelles il existe des indices graves et concordants ;
- les empreintes relevées dans les établissements pénitentiaires afin de s'assurer de l'identité de la personne détenue et d'établir les cas de récidive.

Les données sont conservées vingt-cinq ans maximum pour les empreintes et selon le temps de prescription de l'action publique pour les traces (trois ans pour les délits, dix ans pour les crimes). Au 1er novembre 2010, le faed comptait 3,7 millions de références individuelles. Il a permis de résoudre près de 10 000 affaires en 2010.

3. Le fichier national des empreintes génétiques (fnaeg)

Créé par la loi du 17 juin 1998 relative à la répression des infractions sexuelles ainsi qu'à la protection des mineurs, et mis en œuvre par un décret du 18 mai 2000 (modifié par le décret n° 2009-785 relatif à l'accès d'organisations internationales et d'États étrangers au fichier national automatisé des empreintes génétiques), le fichier national des empreintes génétiques (fnaeg), commun à la police et à la gendarmerie, permet de faciliter la recherche des auteurs d'infractions à l'aide de leur profil génétique ainsi que les personnes disparues et des cadavres non identifiés à l'aide de leur profil génétique, de celui de leurs descendants ou de leurs ascendants. Il s'agit d'un fichier d'identification qui n'a pas pour objectif de conserver les antécédents judiciaires.

Son champ d’application a été élargi en 2001 aux principaux crimes d’atteintes aux personnes et aux biens, puis en 2003, à plusieurs autres domaines de la criminalité. L’enregistrement d’une empreinte génétique dans le fnaeg peut être effectué dans le cadre des infractions limitativement énumérées à l’article 706-55 du cpp, parmi lesquelles figurent notamment les infractions de nature sexuelle, les crimes contre l’humanité et les crimes et délits d’atteinte volontaire à la vie de la personne, de torture et actes de barbarie, de violences volontaires, de trafic de stupéfiants, d’atteintes aux libertés de la personne, de traite des êtres humains, de proxénétisme, d’exploitation de la mendicité et de mise en péril des mineurs.

Le fnaeg est placé sous le contrôle d’un magistrat du parquet hors hiérarchie, assisté par un comité de trois membres tous nommés par le ministre de la Justice.

Les données peuvent être conservées quarante ans pour les condamnés, les personnes décédées, les personnes disparues et les traces et vingt-cinq ans pour les mis en cause et la parentèle des personnes disparues.

Le traité de Prüm, du 27 mai 2005 [7], ratifié par la France à la suite de la loi n° 2007-1160 du 1er août 2007, comporte certaines stipulations en matière de partage d’informations transfrontalières ainsi qu’en matière de terrorisme concernant les fichiers des empreintes génétiques pour lesquels les États parties au traité disposeront désormais, et conformément à leurs législations nationales, d’un accès réciproque automatique.

4. Le fichier des personnes recherchées (fpr)

Le fichier des personnes recherchées (fpr), créé par arrêté du 15 mai 1996 (modifié en 2005), répertorie, au plan national, toutes les personnes faisant l’objet de recherches par l’autorité judiciaire, les services de police, des douanes, les administrations ou les autorités militaires dans le cadre de leurs compétences légales.

Chaque fiche comporte une conduite à tenir en cas de découverte de la personne recherchée, qui énonce des instructions précises aux services de police ou, dans le cadre de la délivrance de documents, aux services administratifs.

L’inscription au fpr peut intervenir dans plusieurs cas de figure : en exécution

d’une décision de justice ou dans le cadre d’une enquête de police judiciaire ; à la demande des autorités administratives (police des étrangers, recherches dans l’intérêt des familles, opposition à sortie du territoire des mineurs, application des mesures administratives relatives au permis de conduire, opposition à délivrance de documents d’identité ou de voyage, etc.) ; à la demande des autorités militaires (déserteurs, insoumis). Un nouveau décret a été publié le 30 mai 2010 (décret n° 2010-569). Les conditions d’inscription au fpr ont été élargies à certaines mesures administratives relatives à la police des étrangers (interdiction d’entrée sur le territoire national). De même peuvent désormais êtres inscrits au fichier les ressortissants d’un État non membre de l’Union européenne faisant l’objet d’une mesure restrictive de voyage, interdisant l’entrée sur le territoire ou le transit par le territoire, adoptée par l’Union européenne ou une autre organisation internationale et légalement applicable en France. Le décret précise également que les services préfectoraux peuvent directement renseigner le fichier sur certaines infractions. Enfin, dans un souci d’amélioration de la sécurité routière et de lutte contre la fraude et la conduite avec un permis invalidé, il a rendu nécessaire d’inscrire dans le fpr les personnes faisant l’objet de recherches en vue de la notification de mesures administratives concernant leur permis de conduire et celles faisant l’objet d’une mesure administrative visant au retrait d’un permis de conduire obtenu indûment. Une nouvelle modification devrait intervenir courant 2011 : la possibilité, sous le contrôle des services de police, de transmettre aux agents de police municipale, agents de police judiciaire adjoints (art. 21 cpp), certaines informations. Au 1er novembre 2010, les services de police ont effectué plus de 51 millions de consultations depuis le 1er janvier 2010 lesquelles ont permis 75 896 découvertes.

VII. Les systèmes de traitement du renseignement judiciaire

Le développement de l’informatique et de la puissance qui y est associée ont permis de faire évoluer les systèmes de traitement de l’information notamment dans le domaine de l’analyse criminelle. Celle-ci est rendue particulièrement nécessaire par la nature complexe (volume important de données, multiplicité des reprises de procédures par des services différents, etc.) et/ou le potentiel sériel de certaines affaires.

Ainsi, grâce à l'informatique, il est aujourd'hui possible de faire des rapprochements rapides entre plusieurs affaires qui seraient traitées par des services différents, dont les faits auraient été commis dans des régions éloignées, mais pour lesquels des similitudes existeraient, par exemple, en matière de mode opératoire. Ces opportunités ont bien entendu pour objectif d'identifier plus rapidement l'auteur d'une infraction sérielle avant qu'il ne commette un nouvel acte.

En créant des fichiers de rapprochement, la France a suivi le chemin des États-Unis et du Canada, car seule l'exploitation complète des données recueillies permet, *a posteriori*, une discrimination entre des personnes (auteurs, complices, témoins ou personnes s'avérant finalement étrangères au dossier) ou entre des éléments matériels (lieux, véhicules, etc.).

Les systèmes de traitement du renseignement judiciaire sont donc des outils de travail indispensables aux investigations policières pour instruire objectivement des dossiers qui peuvent se révéler très lourds. Les éléments de toutes natures (noms, adresses, numéros de téléphone, immatriculations de véhicules, éléments matériels issus des constatations, etc.) et concernant l'ensemble des personnes mentionnées dans une procédure (personnes mises en cause, témoins, victimes) peuvent donc y figurer, dès lors qu'ils sont utiles à la compréhension d'un dossier.

Comme pour les fichiers d'antécédents judiciaires, la loi d'orientation et de programmation de la performance de la sécurité intérieure (lopssi), adoptée le 8 février 2011, consacre les fichiers d'analyse sérielle (nouvel article 230-12 du Code de procédure pénale) : « Afin de rassembler les preuves et d'identifier les auteurs, grâce à l'établissement de liens entre les individus, les événements ou les infractions, des crimes et délits présentant un caractère sériel, les services et unités de la Police et de la Gendarmerie nationales chargés d'une mission de police judiciaire peuvent mettre en œuvre, sous le contrôle des autorités judiciaires, des traitements automatisés de données à caractère personnel. Ces traitements peuvent contenir des données sur les personnes, sans limitation d'âge. » Ces fichiers ne peuvent porter que sur des informations recueillies au cours des enquêtes préliminaires ou de flagrance, sur des investigations exécutées sur commission rogatoire et concernant toute infraction punie d'au moins cinq ans d'emprisonnement, sur des procédures de recherche des causes de la mort prévues par l'article 74 ou de recherche des causes d'une disparition prévues par l'article 74-1 [8].

1. Le système d’analyse et de liens de la violence associée au crime (salvac)

salvac trouve son fondement dans l’article 30 de la loi du 12 décembre 2005 relative au traitement de la récidive des infractions pénales. Il a été autorisé par le décret n° 2009-786 du 23 juin 2009.

La finalité du traitement consiste à opérer des rapprochements entre les procédures judiciaires afin d’identifier et de poursuivre les auteurs de crimes ou délits commis « en série », dans le domaine de la criminalité violente (meurtre, assassinat, acte de torture et de barbarie, viol, agression sexuelle, atteinte sexuelle sur mineur, etc.). L’alimentation et les consultations sont effectuées par 15 policiers et gendarmes de l’Office central pour la répression des violences aux personnes (ocrvp), spécialement habilités et individuellement désignés. Au 1er février 2010, salvac contenait 9 421 dossiers. Il a permis de résoudre 17 affaires sérielles portant sur 120 victimes.

2. anacrim

Le logiciel d’analyse criminelle (anacrim), utilisé par la gendarmerie, est un outil de travail qui fonctionne à partir de fichiers temporaires d’investigations criminelles élaborés exclusivement dans le cadre de procédures judiciaires. Certains services de la Police nationale et d’autres administrations utilisent également ce logiciel.

Le système permet notamment de procéder aux analyses suivantes :

- analyse de cas (étude d’un crime ou d’un délit permettant de situer et de comparer dans le temps les actions des différents protagonistes d’une affaire) ;

- analyse comparative de cas (mise en évidence de relations entre les données disponibles concernant différents crimes et délits analogues) ;

- analyse de profil spécifique (recherche d’éléments permettant de déterminer la personnalité probable du ou des auteurs ayant commis un ou plusieurs

crimes) ;

- analyse de groupe d'auteurs (étude de la structure d'un groupe d'individus connus et des relations entre les membres de ce groupe).

Il a pour finalité principale de mettre en évidence les liens objectifs entre différentes entités (personnes physiques ou morales, lieux, objets, moyens de transport, traces…) afin de relancer des investigations qui, sans cette mise en lumière, pourraient être vouées à l'échec.

3. Le fichier de Lecture automatisée des plaques d'immatriculation (lapi)

Le traitement automatisé de contrôle des données signalétiques des véhicules a été créé, à titre expérimental, par l'arrêté du 2 mars 2007. Il s'agit de traitements destinés à contrôler les données signalétiques des véhicules en prenant la photographie de leurs occupants.

Ils sont mis en œuvre par les services de Police et de Gendarmerie nationales afin de prévenir et de réprimer le terrorisme, de faciliter la constatation des infractions s'y rattachant, de faciliter la constatation des infractions criminelles ou liées à la criminalité organisée au sens de l'article 706-73 du Code de procédure pénale, des infractions de vol et de recel de véhicules volés, des infractions de contrebande, d'importation ou d'exportation commises en bande organisée, prévues et réprimées par le deuxième alinéa de l'article 414 du Code des douanes, ainsi que la constatation, lorsqu'elles portent sur des fonds provenant de ces mêmes infractions, de la réalisation ou de la tentative de réalisation des opérations financières définies à l'article 415 du Code des douanes. Ils sont également mis en œuvre par les services de Police et de Gendarmerie nationales, à titre temporaire, pour la préservation de l'ordre public, à l'occasion d'événements particuliers ou de grands rassemblements de personnes, par décision de l'autorité administrative. Le traitement a été autorisé par un arrêté du 18 mai 2009.

4. Plate-forme d'harmonisation, d'analyse, de recoupement et d'orientation des

signalements (pharos)

Créé par un arrêté du 16 juin 2009, Pharos est tout d'abord un site Internet permettant aux utilisateurs et acteurs d'Internet, et notamment aux internautes, fournisseurs d'accès et services de veille étatiques, de signaler, sans préjudice du respect dû aux correspondances privées, à l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication, des sites ou des contenus contraires aux lois et règlements diffusés sur Internet. Il inclut également un traitement automatisé de données à caractère personnel mis en œuvre par cet Office central et destiné à traiter les signalements transmis par les utilisateurs et acteurs d'Internet. Pharos a pour finalité de recueillir, de manière centralisée, l'ensemble des signalements, d'effectuer des rapprochements entre eux et de les orienter vers les services enquêteurs compétents en vue de leur exploitation.

Les données à caractère personnel enregistrées sont les nom et prénom de l'auteur du signalement, son adresse, son numéro de téléphone et son adresse de messagerie électronique et l'identité du ou des agents ayant traité le signalement. Les données à caractère personnel mentionnées sont conservées deux ans à compter de leur enregistrement. L'adresse ip de l'auteur du signalement est conservée deux ans à compter de son enregistrement.

5. Le fichier Outil de centralisation et de traitement opérationnel des procédures et des utilisateurs de signatures (octopus)

Le fichier octopus, géré par la préfecture de police, constitue un outil utilisé par les fonctionnaires de police de la cellule tags de la centralisation et de traitement opérationnel des procédures et des utilisateurs de signatures direction urbaine de la police de proximité pour constater les infractions réprimées par les articles 322-1 (2e alinéa) et R. 635-1 du Code pénal, c'est-à-dire « le fait de tracer des inscriptions, des signes ou des dessins, sans autorisation préalable, sur les façades, les véhicules, les voies publiques ou le mobilier urbain », rassembler les preuves de ces infractions et rechercher leurs auteurs.

À cette fin, ce fichier permet l'établissement de synthèses de faits et des recoupements (identiques ou/et dus à un même auteur) et l'identification des auteurs de dégradation. Le fichier sera prochainement déclaré dans la cadre de l'article 11-*ter* de la loppsi.

VIII. Les fichiers d'identification administrative

Les fichiers d'identification administrative, tout comme les fichiers administratifs, sont des systèmes techniquement neutres permettant notamment l'établissement de titres d'identité ou de permis de conduire.

1. Le fichier relatif à la carte nationale d'identité

Le fichier relatif à la carte nationale d'identité (décret n° 55-1397 du 22 octobre 1955 et notamment ses articles : 6-8-9-10-11-12) est mis en œuvre par la direction des Libertés publiques et des Affaires juridiques (dlpaj) du ministère de l'Intérieur.

2. Le fichier relatif aux passeports

Le fichier relatif aux passeports (Delphine et tes), créé par le décret n° 2005-1726 du 30 décembre 2005 modifié est également géré par la dlpaj. Il a pour finalité la mise en œuvre des procédures d'établissement, de délivrance, de renouvellement et de retrait des passeports et pour objectif subséquent de prévenir et de détecter leur falsification et leur contrefaçon.

Ce fichier ou traitement est centralisé et mis à la disposition des services de l'État chargés de la délivrance des passeports.

Conformément à l'application du règlement (ce) n° 2252/2004 du 13 décembre 2004 du Conseil de l'Union européenne, les passeports biométriques ont

commencé à être délivrés à compter du 1er janvier 2009. Le décret nº 2008-426 du 30 avril 2008 modifiant le décret nº 2005-1726 du 30 décembre 2005 prévoit que, le traitement dénommé Titres électroniques sécurisés (tes), permettant l'enregistrement de l'image numérisée du visage et des empreintes digitales et celui des pièces du dossier de demande, sera mis en fonction de façon progressive à partir de 2009.

3. Le fichier de suivi des titres de circulation délivrés aux personnes sans domicile ni résidence fixe (sdrf)

Le sdrf, géré par la gendarmerie, a pour finalité le suivi des titres de circulation délivrés aux personnes circulant en France sans domicile ni résidence fixes et qui sont soumises aux dispositions de la loi nº 69-3 du 3 janvier 1969. Ainsi, les personnes sans domicile ni résidence fixes depuis plus de six mois, âgées de plus de 16 ans, doivent, pour pouvoir circuler en France, être munies d'un titre de circulation délivré par les préfectures ou les sous-préfectures, qu'elles souhaitent ou non exercer une activité ambulante.

4. Le fichier national du permis de conduire (fnpc)

Le service du fichier national des permis de conduire, créé par arrêté du ministre de l'Intérieur le 20 décembre 1972, gère l'application réglementaire système national des permis de conduire (snpc). Le service du fnpc a donc pour vocation, en application de l'article L. 225-1 du Code de la route, d'enregistrer et de gérer toutes les informations relatives aux permis de conduire, en particulier les droits de conduire de tout conducteur, ainsi que toutes les informations nécessaires à cette gestion.

Sont, par exemple, enregistrées les décisions administratives, dûment notifiées, prises sur avis de la commission médicale, et portant restriction, maintien, prorogation ou annulation, d'une ou plusieurs catégories du permis de conduire ou encore les mesures dûment notifiées, en tant qu'elles portent avertissement,

rétention, suspension ou interdiction de délivrance du permis de conduire, ainsi que les renseignements relatifs à la notification et à l'exécution de ces mesures.

Une nouvelle application devrait être opérationnelle en 2011-2012. Elle offrira une meilleure qualité de service aux usagers et permettra un renforcement de la lutte contre la violence routière, contre la fraude et le contournement des mesures restrictives prises au niveau national.

IX. Les fichiers « internationaux »

1. Le système d'information Schengen (sis)

Le système d'information Schengen (sis), créé par la Convention d'application de l'accord de Schengen du 19 juin 1990, est un fichier commun à l'ensemble des États membres de l'« espace Schengen », qui a pour objet de centraliser et de faciliter l'échange d'informations détenues par les services chargés de missions de police afin de préserver l'ordre et la sécurité publics. Ce fichier est présenté comme une mesure compensatoire à la suppression des contrôles aux frontières intérieures des États participants et à la libre circulation des personnes.

Le sis, composé d'un système central installé à Strasbourg et de systèmes nationaux – « reflets » de la base centrale – implantés dans chaque pays, comporte deux grandes catégories d'informations : l'une concerne des personnes recherchées, placées sous surveillance ou jugées « indésirables » dans l'« espace Schengen » (art. 95 à 99 de la Convention), l'autre concerne des véhicules ou des objets recherchés (art. 100 de la Convention).

En France, c'est la direction générale de la police nationale, et en particulier la direction centrale de la Police judiciaire, qui est chargée de gérer ce fichier.

Le sis est alimenté, depuis 1995, par le fichier des véhicules volés (fvv) et par certaines fiches du fichier des personnes recherchées (fpr – notamment celles relatives à des mandats d'arrêt et à des exécutions de jugement).

Depuis 1999, les armes, les documents d'identité et les billets de banque saisis dans la base nationale du stic et auxquels est associé le qualifiant « volé », sont automatiquement enregistrés dans le sis.

Le sis II (nouvelle version informatique du fichier SIS 1 + actuel) devrait probablement être mis en œuvre en septembre 2009, et inclure pour les 25 États membres de l'espace Schengen [9] (9 nouveaux États membres entrés dans l'ue en 2004 ont rejoint l'« espace Schengen » en mars 2008, suivis de la Suisse en décembre 2008) de nouvelles catégories d'objets (bateaux, aéronefs, équipements industriels, moteurs de bateaux, containers, moyens de paiement), des liens entre les signalements et introduire des données biométriques.

2. Le fichier Europol

Europol a été créé en vue d'améliorer la coopération policière entre les États membres pour lutter contre le terrorisme, le trafic illicite de drogues et les autres formes graves de la criminalité internationale. C'est l'acte du Conseil, du 26 juillet 1995, qui porte établissement de la convention sur la création d'un Office européen de police (convention Europol).

Il a pour mission d'améliorer l'efficacité des services compétents des États membres et leur coopération dans des domaines de plus en plus nombreux : terrorisme ; trafic illicite de stupéfiants, d'êtres humains, de véhicules ; immigration clandestine ; lutte contre le faux-monnayage et le blanchiment d'argent.

Europol remplit en priorité les fonctions suivantes : faciliter l'échange d'informations entre les États membres ; rassembler et analyser les informations et renseignements ; communiquer aux services compétents des États membres les informations les concernant et les informer immédiatement des liens constatés entre des faits délictueux ; faciliter les enquêtes dans les États membres ; gérer des recueils d'informations informatisés.

En vue de remplir ses fonctions, Europol gère un système d'informations informatisé. Alimenté directement par les États membres, le système d'informations est directement accessible, en consultation, aux unités nationales, aux officiers de liaison, aux directeurs et directeurs adjoints, ainsi qu'aux agents d'Europol dûment habilités.

Outre des données à caractère non personnel peuvent également figurer dans ce système d'informations des données à caractère personnel. Tout fichier automatisé de données à caractère personnel doit faire l'objet, de la part

d’Europol, d’une instruction de création soumise à l’approbation du conseil d’administration. Les données à caractère personnel extraites du système d’informations ne peuvent être transmises ou utilisées que par les services compétents des États membres pour prévenir et lutter contre la criminalité relevant de la compétence d’Europol, et contre les autres formes graves de criminalité.

Toute personne désirant accéder aux données la concernant, stockées à Europol, peut formuler gratuitement une demande dans tout État membre de son choix à l’autorité nationale compétente, qui saisit alors Europol et avise le requérant qu’Europol lui répondra directement. Toute personne est en droit de demander à Europol de rectifier ou d’effacer des données erronées la concernant.

Une autorité de contrôle commune indépendante est chargée de surveiller l’activité d’Europol afin de s’assurer que le stockage, le traitement et l’utilisation des données dont disposent les services d’Europol ne portent pas atteinte aux droits des personnes.

Les deux principaux outils d’Europol sont le système informatisé de données, l’eis, basé à La Haye, alimenté par les États membres et Europol ainsi que les fichiers d’analyse thématiques dédiés aux activités d’organisations criminelles ou des filières d’immigration clandestines.

À l’initiative de l’autorité de contrôle commune d’Europol (acc) une première conférence a réuni à Bruxelles, le 17 octobre 2006, de nombreux acteurs concernés par l’avenir d’Europol. Le débat présidé par le commissaire de la cnil siégeant au sein de l’acc d’Europol a notamment porté sur l’évaluation du niveau de la protection des données dans le cadre des activités d’Europol. Lors du débat, le conseil a exposé le rôle central qui sera dévolu d’ici 2010, à la future agence européenne Europol. Celle-ci sera au cœur de l’échange d’informations et gérera de futures bases de données européennes (adn y compris). Europol a insisté sur le besoin de disposer, dans ce contexte, « d’une information de qualité et à valeur ajoutée » qui ne leur parviendrait pas sans protection des données ni confiance mutuelle. Le vice-président de la commission a alors pleinement concédé la nécessité d’un renforcement du niveau de protection des données dans un cadre juridique relevant du troisième pilier.

X. Les futurs fichiers

Les technologiques de l'information et les capacités informatiques évoluent de plus en plus rapidement. Mais, quand un particulier peut changer son ordinateur personnel au bout de deux ans, la puissance publique ne peut modifier ses systèmes que de manière progressive et à un rythme bien plus lent. Entre les délais liés au développement des systèmes, ceux concernant les spécifications techniques, ceux liés aux contraintes d'examen juridiques et les obligations relatives aux marchés publics, il peut s'écouler des années avant que de nouveaux systèmes de traitement de l'information puissent être mis en œuvre.

Pourtant, afin d'accroître son efficacité et ses capacités de réponse aux évolutions de la criminalité, l'administration a besoin de la modernisation et de l'adaptation de ses outils et en particulier de ses systèmes d'information. Plusieurs projets de développement ou de mise à jour de nouveaux fichiers sont actuellement en cours et devraient être opérationnels d'ici 2012.

Dans le cadre de la loppsi, un chapitre a été consacré aux fichiers de police judiciaire afin d'en poser le cadre juridique. Les fichiers d'antécédents, d'analyse sérielle ou encore de rapprochements judiciaires (art. 230-20 et suivants du Code de procédure pénale) sont désormais autorisés de manière générique sans, bien entendu, supprimer la déclaration et l'examen à la cnil.

1. Le traitement « préplainte en ligne »

Le traitement de données « préplainte en ligne » (ppl) est un dispositif actuellement en cours d'expérimentation dans les départements des Yvelines et de la Charente-Maritime pour une durée de douze mois maximum (décret n° 2008-1109 du 29 octobre 2008). Il s'agit d'un téléservice susceptible de permettre à la victime ou son représentant d'effectuer une déclaration en ligne pour les seuls faits d'atteintes aux biens contre auteur inconnu, d'une part, et d'obtenir un rendez-vous auprès d'un service de Police ou d'une unité de Gendarmerie nationales de son choix pour signer sa plainte, d'autre part. Ce dispositif est d'abord destiné à améliorer les conditions d'accueil du public, dès lors qu'il devrait permettre de limiter les délais d'attente auxquels sont actuellement confrontées les victimes lorsqu'elles se rendent au commissariat ou au sein d'une brigade de gendarmerie pour y déposer plainte. Il devrait également contribuer à réduire le temps nécessaire à l'enregistrement de la plainte par les personnels de police ou de gendarmerie.

2. Le fichier des objets et véhicules signalés (foves)

Projet de modernisation conjointement mené par la Gendarmerie et la Police nationales, l'application foves doit fusionner les applications fos (fichier des objets signalés), fvv (fichier des véhicules volés) ainsi que le stic (système de traitement des infractions constatées) dans sa partie « objets ». Elle constitue un fichier dit de contrôle en présence des objets et véhicules afin de savoir si ceux-ci ont été signalés ou volés auprès des forces de police. Le déploiement est prévu en deux lots successifs, « objets » et « véhicules », et a débuté au second semestre 2009.

3. Le système de traitement des images des véhicules volés (stivv)

La création du « contrôle-sanction automatisé » a entraîné la mise en place de la cellule de traitement des images des véhicules volés (ctivv) au sein du service technique de Recherches judiciaires et de Documentation (strjd) implanté à Rosny-sous-Bois (93). Son outil est le système de traitement des images des véhicules volés (stivv). Cette cellule, à vocation interministérielle, a pour mission d'exploiter, à des fins d'enquêtes judiciaires, les photographies prises par des radars automatisés de véhicules volés, ou mis sous surveillance, ou circulant avec une immatriculation fausse ou altérée. Elle est également chargée de confirmer ou d'infirmer auprès du Centre automatisé de constatation des infractions routières (cacir) la situation administrative ou judiciaire des véhicules au moment de la commission de l'infraction.

4. L'application judiciaire dédiée à la révélation des crimes et délits en série (ajdrcds)

ajdrcds est un traitement informatique qui s'adosse à la démarche de rapprochement judiciaire habituellement utilisée dans la pratique professionnelle

de l’enquêteur. C’est un outil qui vient à l’appui du praticien dans la gestion de la masse croissante d’informations que doit traiter l’enquêteur lors des procédures et des affaires complexes.

La finalité d’ajdrcds est de faciliter la détection de crimes et délits de même nature imputable à un même auteur ou groupe d’auteurs ainsi que la détection des infractions ou des comportements délinquantiels poly-morphes réitérés par un même auteur ou groupe d’auteurs.

La recherche serait réalisée à partir de la sélection des faits constatés par la Police et la Gendarmerie nationales dans la future base traitement des procédures judiciaires (fusion de stic et judex), par leur enrichissement au moyen d’autres données contenues dans les procédures judiciaires et par celles issues de toutes les sources d’informations disponibles pour les enquêteurs (messagerie opérationnelle, fichiers, sources ouvertes).

ajdrcds est en phase de conception. Sa mise en œuvre suppose la modification préalable de l’article 21-1 de la loi du 18 décembre 2003 modifiée et l’élaboration consécutive d’un décret pris après avis de la cnil. Il devrait se voir autoriser dans la cadre de l’article 11 ter de la loppsi.

La puissance opérationnelle de cet outil a conduit le groupe de contrôle sur les fichiers à recommander une utilisation limitée de celui-ci aux faits d’une particulière gravité. Le ministre de l’Intérieur s’est déclaré favorable à l’introduction d’un seuil d’infraction pénale à partir duquel de tels rapprochements pourront être traités informatiquement (infractions punies de plus de cinq ans d’emprisonnement).

5. L’application Cellule opérationnelle de rapprochement et d’analyse des infractions liées (corail)

Mise en place en 2006 à la direction de la Police judiciaire de la préfecture de police, corail a pour objet principal la mutualisation des diffusions d’informations opérationnelles auprès des enquêteurs (télégrammes via le réseau de commandement [rescom], circulaires d’information et de recherche diffusées par la police judiciaire). corail permet également de suivre et de traiter les

gardes-à-vue au sein d'un service.

Les informations enregistrées et diffusées sont :

- les données issues des télégrammes d'informations diffusés par le rescom (signalement des faits commis ou élucidés) ;
- les données issues des mains courantes d'informations ;
- les données d'affaires ou de synthèse correspondant à un résumé des faits ou de la procédure (dates, lieux, nombre d'auteurs, résumé de l'affaire, référence, service saisi, etc.) ;
- les données photographiques (photographie de suspect, portrait-robot, photographie d'objet) ;
- les données de garde à vue (identité de la personne, nature de l'infraction, nom de l'opj, etc.).

Ces données se présentent sous forme de fiches se rapportant à des faits, sous forme d'états opérationnels regroupant des faits de même nature ou commis dans la même zone géographique, ou encore sous forme de synthèses opérationnelles rassemblant des faits présentant des similitudes de mode opératoire.

corail, actuellement en phase d'expérimentation au sein des drpj de Paris et de Versailles, sera généralisé en 2011 à l'ensemble des services territoriaux d'investigation de police judiciaire et de sécurité publique. Il devrait faire l'objet d'une déclaration dans le cadre de l'article 11 *ter* de la loppsi.

6. Traitement des procédures judiciaires (tpj – ex ariane)

Début 2005, la Gendarmerie et la Police nationales, qui sont depuis le 1er janvier 2009 placées sous la tutelle unique du ministère de l'Intérieur, confrontées à la nécessité de moderniser leurs systèmes respectifs judex et stic, se sont associées pour réaliser un nouveau fichier commun de recherches et de rapprochements criminels : traitement des procédures judiciaires (tpj – ex-ariane).

Cette coopération opérationnelle et technique s'inscrit dans le sens de la loi d'orientation et de programmation pour la sécurité intérieure d'août 2002 (lopsi) qui prescrit le rapprochement des grands fichiers informatisés des deux forces.

Outre les avantages attendus en termes de rationalisation des moyens techniques et financiers nécessaires à sa réalisation, le nouveau système permettra l'accès pour tout gendarme ou policier à l'ensemble des informations relatives aux enquêtes judiciaires quel que soit le service ou l'unité à l'origine de leur enregistrement. La mise en œuvre opérationnelle devrait intervenir au second semestre 2011.

Les informations contenues dans tpj respecteront les mêmes règles que les applications stic et judex actuelles. Deux nouvelles catégories de données seront intégrées au système : les morts suspectes et les disparitions inquiétantes (art. 74 et 74-1 du Code de procédure pénale).

Les règles actuelles valables pour les applications stic et judex seront appliquées pour tpj et ouvertes, sous certaines conditions aux services de la douane judiciaire. Il est également prévu d'organiser l'accès direct effectif, déjà prévu par le législateur, au profit des parquets au titre du contrôle de la régularité du fichier. tpj sera alimenté par lrppn et lrpgn. tpj permettra de regrouper l'ensemble des procédures judiciaires en vue de leur transmission automatique, et de leur mise à jour, au système Cassiopée du ministère de la Justice et des Libertés.

7. Base de données de sécurité publique (bdsp – ex athen @)

Devant remplacer le système aramis, la Gendarmerie nationale a créé son traitement de données lié au renseignement de proximité à travers quatre modules relatifs aux traitements « ordre public ». Le module gispap est une copie conforme du fichier pasp de la Police nationale. Le module Gestion des événements d'ampleur (gea) permettra de recueillir des informations sur le déroulement des événements majeurs et les conduites à tenir. Le module Gestion des sollicitations et des interventions (gsi) est destiné à recueillir, à apporter des réponses adaptées aux sollicitations des usagers et à conduire l'engagement des personnels et des moyens de la gendarmerie dans les meilleures conditions de

sécurité. Ainsi, par exemple, si lors d'une intervention une brigade est face à une personne en possession d'une arme, celle-ci pourra être inscrite dans ce fichier afin que, dans le cas d'une nouvelle intervention, l'équipage soit averti de cet élément. L'inscription dans ce fichier ne pourra être réalisée qu'*a posteriori* d'une première intervention et non *a priori*. Enfin, le module Sécurisation des interventions et demandes particulières de protection (sidpp) a pour finalité de collecter des données destinées à prévenir les risques encourus lorsque les forces de gendarmerie sont appelées à intervenir à l'égard de personnes dont la dangerosité ou l'agressivité a été déjà constatée lors d'une précédente intervention. Il ne s'agit donc que d'un fichier des incidents recensés.

8. Logiciel d'uniformisation des prélèvements et identification (lupin)

Le traitement lupin est actuellement en cours d'expérimentation à la préfecture de police de Paris. C'est un système de traitement du renseignement judiciaire visant à lutter contre les cambriolages et les vols en procédant à des rapprochements à partir des données de police technique et scientifique et relatives aux modes opératoires recueillies sur les scènes d'infraction. Il s'agit donc de pouvoir mettre en exergue le caractère sériel de ce type d'infraction. La durée de conservation des données actuellement proposée est de cinq ans. Il devrait être déclaré sur la base de l'article 11 *ter* de la loppsi.

9. Fichiers de travail de police judiciaire des unités de recherches de la gendarmerie nationale

Un décret devrait être pris en 2011 afin de couvrir l'ensemble des traitements locaux des unités de recherche de la gendarmerie (11 % des unités territoriales). Ces traitements ont pour finalité de faciliter la constatation des infractions à la loi pénale, le rassemblement des preuves de ces infractions au cours des enquêtes préliminaires ou de flagrance ou des investigations exécutées sur commission rogatoire ou au cours des procédures de recherche de cause de la mort ou de blessures, ou des causes de disparition inquiétante, ainsi que la

recherche de leurs auteurs. Ces traitements stockent uniquement des messages, télégrammes, avis, fiches, synthèses, rapports ou comptes rendus relatifs à des phénomènes de délinquance ou criminalité. Ils peuvent contenir des données sur les personnes à l'encontre desquelles il existe des raisons plausibles de soupçonner qu'elles aient pu participer, comme auteurs ou complices, à la commission d'un crime ou délit ou contravention (l'enregistrement des données concernant ces personnes peut intervenir, le cas échéant, après leur condamnation pour un crime ou délit) ou faisant l'objet d'une enquête ou d'une instruction pour recherche des causes de la mort ou de blessures, prévue par l'article 74 du Code de procédure pénale, ou d'une enquête ou d'une instruction pour recherche des causes d'une disparition inquiétante ou suspecte, prévue par les articles 74-1 et 80-4 du même Code. Des durées de conservation de trois à vingt ans sont prévues. Les mineurs peuvent y être enregistrés. Les traitements ne font l'objet d'aucune interconnexion, aucun rapprochement ni aucune forme de mise en relation avec d'autres traitements ou fichiers.

Un recensement encore à parfaire

Suite aux recommandations du groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie, les directions générales de la Police et de la Gendarmerie nationales ont entrepris fin 2010 une démarche qualité visant notamment à recenser, de manière exhaustive, l'ensemble des traitements automatisés de données à caractère personnel, qu'ils soient locaux ou qu'ils aient été créés par des services centraux comme, par exemple, les fichiers des fourrières et immobilisations, le fichier des contrôles judiciaires, le fichier des cercles de jeux, etc.

Notes

[1] Régularisés par arrêté du 30 mai 2011 (*JO* du 06/08/2011).
[2] Régularisés suite à l'adoption de la loppsi du 08/02/2011.
[3] Les armes sont classées selon différentes catégories dans le Code de la défense nationale (art. L. 2331-1). Le port, le transport et l'usage d'une arme sont réglementés en fonction de la catégorie à laquelle appartient l'arme.

[4] Il existe trois services militaires de renseignements : la direction générale de la Sécurité extérieure (dgse) qui dépend du ministère de la Défense, la direction du Renseignement militaire (drm) qui est rattaché au chef d'état-major des armées et la direction de la Protection et de la Sécurité de la défense (dpsd) qui dépend du cabinet du ministre de la Défense.
[5] Le 15 Juin 2011, le directeur de cabinet du ministre de l'Intérieur indiquait au président du Groupe de contrôle qu'il « demandait à ses *services d'entamer les procédures visant à la modification des décrets pasp et gipasp afin de sortir la mention "origines géographiques" des données sensibles et de ne permettre l'enregistrement de données factuelles strictement limitées à l'origine géographique, au lieu de naissance, à la nationalité ou à la dénomination commune de la bande selon ses propres critères* ».
[6] Voir *Fichiers de police et de gendarmerie. Comment améliorer leur contrôle et leur gestion ?*Collection des rapports officielsParis, La Documentation française, mars 2006
[7] Le traité de Prüm (également appelé « Schengen III » ou « Schengen plus ») a été signé entre sept États membres de l'Union européenne (ue) : la Belgique, l'Allemagne, l'Espagne, la France, le Luxembourg, les Pays-Bas et l'Autriche.
[8] Dans sa décision du 10 mars 2011, le Conseil constitutionnel a, dans un considérant interprétatif (n° 71), limité les possibilités offertes par les fichiers d'analyse sérielle en indiquant que « ces logiciels ne pourront conduire qu'à la mise en œuvre, autorisée (par le juge d'instruction ou le procureur), de traitements de données à caractère personnel particuliers, dans le cadre d'une enquête ou d'une procédure déterminée portant sur une série de faits et pour les seuls besoins de ces investigations ».
[9] Le Royaume-Uni, l'Irlande et Chypre attendent le démarrage effectif du SIS II pour se connecter au système d'information Schengen et devenir opérationnels. Le Lichtenstein devrait rejoindre le système d'information en décembre 2009.

Chapitre III

Contrôle et libertés

La réglementation française sur la création et l'utilisation des fichiers nominatifs informatisés de données à caractère personnel est née des craintes suscitées par l'informatisation croissante de notre société et des possibilités puissantes que celle-ci ouvrait en matière de traitement et de croisement des informations, notamment à caractère nominatif.

I. Une histoire douloureuse

Si les fichiers de police ont toujours existé (clandestins, manuels, politiques, etc.), la France entretient une relation douloureuse avec la question des fichiers, certaines affaires ayant profondément marqué l'opinion publique et l'inconscient collectif.

1. L'affaire des fiches (dite « des casseroles »)

Nommé ministre de la Guerre en 1900, le général Louis André souhaite « républicaniser » et laïciser l'armée et décide de faire établir des fiches sur les opinions politiques et religieuses des officiers. Doutant de la loyauté du service de Renseignement de l'armée (le 2e bureau) discrédité suite à l'affaire Dreyfus, il choisit de confier cette opération de police secrète aux loges maçonniques du Grand Orient de France qui est à l'époque totalement engagé dans la lutte pour la séparation de l'Église et de l'État.

Environ 19 000 fiches sont ainsi centralisées au secrétariat du Grand Orient de France avant d'être transmises au cabinet du ministre de la Guerre. L'avancement des officiers devient conditionné au contenu de leur fiche.

Les scrupules du secrétaire général du Grand Orient le conduisent à céder un lot de fiches et toutes les demandes de renseignements formulées par le cabinet du ministre à Jean Guyot de Villeneuve, un ancien officier d'état-major élu député. Ce dernier provoque le scandale en interpellant le Gouvernement à la chambre le 28 octobre 1904. Cette affaire et la polémique qu'elle engendre entraînent la chute du Gouvernement, mais la politique de « républicanisation » du personnel de l'État (et donc de l'armée) se poursuivra.

2. La mise en fiche des Juifs durant la Seconde Guerre mondiale

Le 27 septembre 1940, une ordonnance édictée par l'occupant allemand impose à la population juive de la zone occupée de se faire recenser auprès des commissariats de police ou des sous-préfectures. Le service du fichier juif (ou service « Tulard », du nom de son chef) est alors spécialement créé à la préfecture de Police. Sa mission consiste à centraliser les déclarations, à établir et à classer les fiches selon quatre ordres (alphabétique, nationalité, domicile et profession). André Tulard s'acquitte de cette mission avec un zèle prononcé. Il crée un fichier sophistiqué, autorisant différents modes de consultation, là où les autorités allemandes ne demandent, d'un point de vue pratique, qu'un simple registre.

Le même fichier est mis en place pour la zone libre quelques mois plus tard. Le 2 juin 1941, après avoir défini le statut des Juifs, le maréchal Pétain ordonne leur recensement. Ainsi, toute personne juive aux termes de la loi doit formuler une déclaration écrite auprès de son préfet ou sous-préfet. Bâti sur le modèle du fichier de la préfecture de Police, le fichier de la direction générale de la Police nationale est créé. Il peut lui aussi être consulté selon plusieurs modes : par ordre alphabétique, par nationalité, par profession et par lieu de domicile. Les sociétés juives, qu'elles soient françaises ou étrangères, sont elles aussi dénombrées. Une circulaire du secrétaire d'État à l'Intérieur, Pierre Pucheu, explique même scrupuleusement aux préfets la manière dont doivent être établies les fiches.

En 1941, ce sont ainsi près de 300 000 déclarations qui sont formulées (155 000 en zone occupée et 140 000 en zone libre) et donc tout autant de juifs qui sont fichés. Les fichiers ainsi constitués vont être utilisés dans le cadre des arrestations ou des rafles. Ainsi, pour la rafle des 16 et 17 juillet 1942, restée

célèbre sous le nom de « rafle du Vel d'Hiv », les fiches d'environ 27 000 juifs sont remises à la direction de la Police municipale parisienne, chargée de procéder aux arrestations. D'après le 3e rapport de la cnil, en 1980, les fichiers créés sous l'Occupation auraient été détruits sans toutefois que la preuve en fut rapportée, ce qui fait dire au rapporteur de la cnil qu'il « subsiste de larges zones d'ombre » sur leur devenir.

Durant la Seconde Guerre mondiale, les populations juives ne seront pas les seules à faire l'objet d'un fichage. Ainsi, la franc-maçonnerie doit aussi faire face à une double hostilité : celle du régime pétainiste et celle de l'occupant allemand. La répression antimaçonnique est l'une des illustrations les plus concrètes de la collaboration. C'est le service des sociétés secrètes, créé par Vichy à l'automne 1940, infiltré par les Allemands, qui, outre les opérations de propagande antimaçonnique, sera chargé de l'élaboration de la liste des francs-maçons et de la mise en place d'un important fichier auquel le service de contre-espionnage allemand (le Sicher Heitsdienst, installé au siège du Grand Orient, rue Cadet) aura accès et qui lui facilitera les arrestations perquisitions et saisies de biens.

Les homosexuels durent également subir la répression du régime nazi en Allemagne. Dès mars 1934, les premières rafles d'homosexuels débutent en Allemagne sur la base du Code pénal et du § 175 qui condamnait de trois à cinq ans de prison la sexualité entre hommes. En France, au début des années 1920, les services de police renforcent leur surveillance des mœurs. Des fichiers vont être constitués et seront remis aux nouvelles autorités nationales-socialistes dans le Haut-Rhin, le Bas-Rhin et la Moselle et contribueront à l'identification et à la déportation de centaines d'homosexuels.

3. Le projet safari (système automatisé pour les fichiers administratifs et le répertoire des individus)

Dans son édition du 21 mars 1974, le journal *Le Monde* publie un article signé par Philippe Boucher et intitulé « safari ou la chasse aux Français ». L'auteur fait part de la double crainte que lui inspire l'ordinateur Iris 80 loué par le ministère de l'Intérieur. Il s'agit en effet de la machine la plus puissante du constructeur

national cii (Compagnie internationale pour l'informatique).

Ce nouvel ordinateur suscite alors l'inquiétude et ravive les peurs d'un État policier qui aurait alors les moyens de contrôler la population à travers les informations personnelles qu'il aurait alors en sa possession. Ce système permettrait également d'accéder à des informations détenues par d'autres administrations. En effet, l'insee vient alors d'achever l'informatisation du répertoire national des personnes physiques, dans lequel chaque individu est identifié par un numéro à 13 chiffres, et prévoit la fusion de tous les fichiers des administrations en utilisant ce numéro à 13 chiffres comme identifiant unique. Ce nouveau fichier unique serait baptisé système automatisé pour les fichiers administratifs et le répertoire des individus (safari).

Face à la campagne de presse qui suit la parution de l'article de Philippe Boucher, le Premier ministre décide d'interdire toute interconnexion de fichiers et crée une commission d'enquête baptisée « Informatique et Libertés » et présidée par Bernard Chenot. Le rapport issu des travaux de la Commission en 1975 servira de base par la suite au Parlement pour le vote de la loi « Informatiques et Libertés » du 6 janvier 1978, créant notamment la Commission nationale de l'informatique et des libertés.

II. Une protection constitutionnelle

Le Conseil constitutionnel a reconnu la valeur constitutionnelle de la protection des données personnelles en la rattachant tout d'abord au principe de la liberté personnelle dans le cadre de l'examen de la loi portant adhésion de la France à la convention d'application Schengen [1]. À cette occasion, il juge que la Convention comporte un dispositif de protection suffisant de nature à assurer le respect de la liberté personnelle en cas d'exploitation ou d'utilisation des catégories de données enregistrées dans le système d'information Schengen.

Puis, dans sa décision du 13 mars 2003 [2], suite à l'examen des recours portant sur la loi sur la sécurité intérieure, le Conseil constitutionnel a considéré « qu'il appartenait au législateur d'assurer la conciliation entre d'une part, la sauvegarde de l'ordre public et la recherche des auteurs d'infractions, toutes deux nécessaires à la protection de principes et de droits de valeur constitutionnelle, et, d'autre, part, le respect de la vie privée ». En 2004, lors de l'examen de la constitutionnalité du fichier judiciaire national automatisé des auteurs

d’infractions sexuelles, il a de nouveau fait référence au droit au respect de la vie privée [3].

Par ailleurs, dans sa décision du 20 janvier 1993 [4], le Conseil constitutionnel consacre la valeur accordée à la loi du 6 janvier 1978 en la qualifiant notamment de loi protectrice des libertés individuelles. Dans plusieurs décisions, le respect des dispositions de la loi « Informatique et Libertés » est apparu comme une condition nécessaire à la validité constitutionnelle des textes examinés. Toutefois, la loi du 6 janvier 1978 n’a pas valeur constitutionnelle et le législateur peut la modifier, la compléter ou la mettre à jour [5].

Le fait de faire référence aux libertés personnelles et non aux libertés individuelles entraîne une double compétence juridictionnelle : administrative et judiciaire, et non exclusivement judiciaire. Ceci d’autant plus que les recours concernant les décisions de la cnil relèvent du juge administratif. Cependant, et comme l’a aussi rappelé le Conseil constitutionnel dans sa décision de mars 2003, les fichiers de police judiciaire sont sous la responsabilité du procureur de la République, magistrat relevant de l’ordre judiciaire.

III. La loi Informatique et Libertés

Suite aux inquiétudes nées du projet safari, mais plus largement aux nouvelles opportunités offertes par le développement de l’informatique, et à ses conséquences éventuelles sur les libertés individuelles, la nécessité de disposer d’une réglementation équilibrée entre protection des droits individuels et usage de l’informatique s’est fait jour.

Cependant, la loi issue des débats de 1978 ne vise pas exclusivement l’informatique puisque les fichiers classiques manuels, privés ou publics, sont également concernés et ont prouvé, par le passé, qu’ils pouvaient être aussi dangereux pour les libertés. Il n’en demeure pas moins que le développement des nouvelles technologies et la puissance croissante des traitements de l’information donnent une nouvelle dimension à la question de la collecte, du stockage, de l’usage et de la communication des données relatives aux individus.

La loi « Informatique et Libertés » du 6 janvier 1978 édicte tout d’abord un principe général qui n’a pas été remis en cause par la loi du 6 août 2004 : « L’informatique doit être au service de chaque citoyen. Son développement doit

s’opérer dans le cadre de la coopération internationale. Elle ne doit porter atteinte ni à l’identité humaine, ni aux droits de l’homme, ni à la vie privée, ni aux libertés individuelles ou publiques. »

Le texte s’applique également dans deux cas distincts mais cumulables : d’une part, si des données nominatives font l’objet d’une gestion par le biais d’un fichier et cela que ce dernier soit manuel ou mécanographique et, d’autre part, si des données nominatives font l’objet d’un traitement automatisé. Selon le cas, les contraintes imposées par la loi seront plus ou moins importantes. L’existence de données nominatives est donc une condition impérative d’application de la loi.

La loi du 6 août 2004 relative à la protection des personnes physiques à l’égard des traitements de données à caractère personnel, transposant en France la directive européenne 95/46 ce du 24 octobre 1995, a modifié la notion d’« information nominative » qui s’efface au profit de celle de « données à caractère personnel » [6].

De même, la notion de « traitement automatisé » issue de l’article 5 de la loi de 1978 est élargie. Antérieurement, pour la cnil, un traitement automatisé devait s’entendre par toute application informatique finalisée utilisant les fonctions offertes par un système informatique. Elle s’étend désormais à tous les traitements, quel que soit le procédé technique utilisé.

La loi détermine également les conditions de licéité des traitements portant sur le respect des principes de loyauté [7], la limitation de la durée de conservation des données ou encore l’exactitude ces dernières. La loi de 2004 a introduit une nouvelle condition liée au respect du principe de proportionnalité : le traitement ne doit porter que sur des données qui sont « adéquates, pertinentes et non excessives au regard des finalités pour lesquelles elles sont collectées et pour lesquelles elles sont traitées ultérieurement ».

La nouvelle loi précise également les conditions de l’utilisation future des données collectées. Elle pose le principe de l’interdiction de tout traitement ultérieur des données « incompatible avec les finalités pour lesquelles elles ont été collectées » à l’exception des traitements réalisés à des fins statistiques ou à des fins scientifiques ou historiques sous réserve que diverses conditions soient réalisées.

La loi détermine les formalités préalables à la mise en œuvre des traitements (régime de déclaration ou d'autorisation) et fixe les obligations incombant aux responsables de traitements et les droits des personnes.

En cas de non-respect des dispositions légales, des peines de nature correctionnelle (art. 226-16 à 226-24 du Code pénal) mais également des sanctions administratives ou pécuniaires peuvent être prononcées.

Cette loi institue enfin la Commission nationale de l'informatique et des libertés (cnil).

IV. Le rôle de la cnil

Instituée par la loi « Informatique et Libertés » du 6 janvier 1978, la Commission nationale de l'informatique et des libertés (cnil) a vu son mode d'action réformé par la loi du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel. La cnil est une autorité administrative indépendante composée d'un collège pluraliste de 17 personnalités dont 4 parlementaires (2 députés et 2 sénateurs), 2 membres du conseil économique et social, 6 représentants des hautes juridictions et 5 personnalités qualifiées désignées par le Conseil des ministres (3), le président de l'Assemblée nationale (1) et le président du Sénat (1). La cnil élit son président parmi ses membres et ne peut recevoir d'instruction d'aucune autorité. Le budget de la cnil relève toutefois du budget de l'État. Elle emploie 105 personnels. Les décisions de la cnil peuvent faire l'objet d'un recours devant la juridiction administrative.

La cnil est chargée de veiller au respect de la loi « Informatique et Libertés ». Elle a tout d'abord une mission d'information puisqu'elle se doit d'informer les personnes de leurs droits et de leurs obligations : droits accordés aux individus lorsqu'ils se retrouvent enregistrés dans un fichier et obligations pour les personnes morales ou les administrations qui créent, développent ou modifient un traitement de données à caractère personnel.

La cnil peut également proposer au Gouvernement des mesures législatives ou réglementaires visant à renforcer la protection des libertés et le droit de la vie privée face au développement des nouvelles technologies. L'avis de la cnil est obligatoire avant toute transmission au Parlement d'un projet de loi créant un

traitement de données à caractère personnel, ce qui concerne l'ensemble des fichiers de police et de gendarmerie dès lors qu'ils contiennent des données à caractère personnel.

La cnil a également pour mission de garantir l'application des modalités du droit d'accès aux données contenues dans les traitements. Elle exerce, pour le compte des citoyens qui en font la demande, l'accès aux fichiers intéressant la sûreté de l'État, la Défense et la Sécurité publique.

La loi « Informatique et Libertés » a également prévu un régime d'autorisation pour la création de certains fichiers. Antérieurement à la loi de 2004, les formalités de déclaration des fichiers auprès de la cnil étaient différentes selon que le traitement était géré par le secteur public ou le secteur privé. Ainsi, les traitements relevant de l'Administration devaient obtenir un avis favorable de la cnil alors que ceux créés sur initiative du secteur privé n'étaient astreints qu'à une simple déclaration. De plus, dans ce cas, le rôle de la cnil était limité au seul contrôle de « la régularité de la déclaration effectuée auprès d'elle au regard des prescriptions » exigées par la loi. La loi prenait aussi en compte un autre critère : celui relatif à la sensibilité des données pour soit soumettre à autorisation particulière leur traitement (données sur les origines raciales, les opinions philosophiques, religieuses ou politiques), soit prévoir des formalités allégées pour certaines catégories de traitements « courants » et ne portant manifestement pas atteinte à la vie privée et aux libertés.

La loi de 2004 modifie de manière sensible les obligations déclaratives des responsables de traitements. La déclaration devient le régime de droit commun pour la plupart des traitements, et ce, quel que soit le responsable, public ou privé. Cependant, des allégements de formalités sont prévus. Ainsi, ne sont désormais soumis à autorisation ou avis de la cnil, que les seuls traitements présentant des risques particuliers au regard des droits et libertés des personnes. Les fichiers manuels doivent aussi faire l'objet de formalités auprès de la cnil.

La cnil a la possibilité d'édicter des normes permettant d'encadrer les conditions d'utilisation de certaines catégories de traitements « courants » ne portant pas atteinte à la vie privée ou aux libertés. Ceci permet de simplifier les obligations déclaratives des responsables de traitements. Aussi, 70 % des traitements déclarés à la cnil le sont aujourd'hui sous forme simplifiée. La cnil a également la possibilité d'accepter, pour un organisme identifié, une déclaration unique regroupant un ensemble de traitements présentant des finalités identiques ou

liées entre elles.

La loi prévoit également la possibilité d'une exonération de formalités pour certaines catégories de traitements ou sur initiative de la cnil (art. 24). Cette possibilité devrait permettre à la cnil de concentrer ses moyens d'action vers des activités prioritaires comme l'examen des projets sensibles, l'instruction des plaintes ou le développement des contrôles sur place.

Le législateur, lors du vote de la loi de 2004, a décidé de maintenir, pour certaines catégories de traitements sensibles relevant du secteur public (et notamment les fichiers de police et de gendarmerie), un régime de demande d'avis excluant l'application du régime de l'autorisation par la cnil. Il a toutefois exigé la déclaration et la mise en conformité de l'ensemble des fichiers de police et de gendarmerie avant le 24 octobre 2010.

La procédure applicable est déterminée à la fois en fonction de la qualité juridique de l'autorité publique responsable du traitement, de la finalité de celui-ci et de la nature des données enregistrées. Ainsi, par exemple, doivent être autorisés par décret en Conseil d'État, pris après avis motivé et publié de la cnil, les traitements portant sur des données sensibles mis en œuvre pour le compte de l'État qui intéressent la sûreté de l'État, la Défense ou la Sécurité publique ou dont l'objet est la prévention, la recherche, la constatation ou la poursuite des infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté ou encore qui portent sur des données biométriques. La loi de 2004 a donc supprimé, pour ce type de fichiers, l'avis conforme de la cnil ou l'intervention d'un décret en cas d'avis défavorable. L'absence de réponse dans un délai de deux mois équivaut à un avis favorable de la Commission.

Le régime de la demande d'autorisation à la cnil, qui était limitée jusqu'en 2004 aux fichiers de recherche médicale et aux traitements d'évaluation des pratiques de soins, a été étendu à dix catégories de traitements (art. 25) dont, par exemple, les traitements statistiques, automatisés ou non, de données sensibles réalisées par l'insee ou par un service statistique ministériel. À défaut de réponse de la Commission dans un délai de deux mois, la demande est considérée comme étant rejetée.

Le contrôle de la Commission s'opère préalablement à la mise en œuvre des traitements de données mais également *a posteriori*. Ce dernier s'effectue sur place, selon des conditions de temps (de 6 à 21 heures) et de lieu (locaux à usage

professionnel servant à la mise en œuvre d'un traitement de données à caractère personnel, à l'exclusion des parties affectées au domicile privé) fixées par la loi du 6 août 2004.

Les membres et agents de la cnil ont accès aux programmes informatiques et aux données, mais leurs pouvoirs d'investigation connaissent certaines limites. Ainsi, la communication de données médicales ne peut être requise que par un médecin, et les personnes astreintes au secret professionnel ne sont pas tenues de fournir les renseignements demandés dans le cadre des contrôles.

En cas de manquements, la cnil a la possibilité de dénoncer au parquet les infractions à la loi qu'elle constate mais peut également prendre des mesures coercitives et des sanctions (avertissements, mises en demeure, sanctions pécuniaires, injonctions de cesser le traitement, voire interruption temporaire de celui-ci ou verrouillage des données).

V. Le contrôle des magistrats

Certains fichiers de police et de gendarmerie, liés aux missions de police judiciaire, sont soumis au contrôle des magistrats du parquet. Toutefois, compte tenu de leur charge de travail, leur rôle demeure limité, tant en ce qui concerne l'alimentation des fichiers, que pour ce qui est du contrôle effectif des bases de données.

L'article 21 de la loi du 18 mars 2003 a placé les fichiers de police judiciaire sous le contrôle du procureur de la République compétent qui peut demander que les informations enregistrées soient effacées, complétées ou rectifiées, notamment en cas de requalification judiciaire. Ce principe général est une reprise du dispositif mis en place lors de la publication du décret autorisant le stic. Ainsi, pour les deux fichiers d'antécédent judiciaire, stic et judex, le procureur est chargé de transmettre les informations judiciaires pour sa mise à jour : condamnation, relaxe, non-lieu ou absence de poursuites. En cas d'acquittement ou de relaxe, les données nominatives doivent être effacées. En revanche, en cas de non-lieu ou absence de poursuite, les informations nominatives sont conservées sauf si le procureur décide de les faire effacer.

Des fichiers particuliers bénéficient d'un contrôle renforcé de l'autorité judiciaire. Il s'agit notamment du fnaeg qui est placé sous le contrôle d'un

magistrat qui dispose d'un accès permanent au fichier. Ce magistrat est hors hiérarchie et est nommé pour trois ans par arrêté du garde des Sceaux. Le fichier judiciaire national automatisé des auteurs d'infractions sexuelles ou violentes est également placé sous le contrôle du magistrat qui gère le casier judiciaire national.

À la suite d'une des recommandations du Groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie, un référent national, membre du Conseil d'État, a été créé en vue de s'assurer du droit à l'oubli pour les mineurs lorsqu'ils ont fait l'objet d'un enregistrement dans le fichier de prévention des atteintes à la sécurité publique. Il doit ainsi s'assurer de l'effacement, au terme du délai de trois ans prévu dans le décret pasp des données concernant les mineurs (décret n° 2010-1540 du 13 décembre 2010).

La loppsi a également prévu que des magistrats, désignés par le ministre de la Justice et des Libertés, soient spécialement chargés de contrôler la mise en œuvre et/ou la mise à jour des fichiers de police judiciaire (antécédents, analyse sérielle ou rapprochements judiciaires).

VI. Les droits ouverts aux citoyens

La loi « Informatique et Libertés », tout en créant des obligations à la charge du responsable d'un traitement de données, a également imposé le respect de certains droits pour les personnes. Toutefois, les droits ouverts aux citoyens ne concernent pas l'ensemble des traitements et peuvent être limités notamment pour certains fichiers sensibles comme ceux gérés par la Police et la Gendarmerie nationales.

1. Le droit d'information

Pour assurer la loyauté et la liberté de la collecte, mais aussi pour permettre au citoyen d'exercer son droit de contrôle sur les données, il est prévu que les personnes, auprès desquelles doivent être recueillies des informations, doivent être informées de certaines dispositions. C'est ce que l'on appelle le droit d'information. Ainsi, toute personne doit être informée du caractère obligatoire ou facultatif des réponses, des conséquences éventuelles d'un défaut de réponse,

des destinataires des données et de l'existence d'un droit d'accès et de rectification. La loi de 2004 a étendu la nature des informations pouvant être communiquées : identité du responsable du traitement, finalité poursuivie par le traitement, existence d'un droit d'opposition et d'un droit d'accès, transferts de données envisagés à destination d'un État non membre de l'Union européenne. Même lorsque les données n'auront pas été recueillies auprès de la personne, celle-ci devra être informée des conditions d'utilisation de ses données et de ses droits.

Des exceptions à cette obligation d'information sont prévues par la loi, notamment lorsque ces données sont collectées pour la prévention, la recherche ou la poursuite d'infractions pénales. La loi permet également de limiter si nécessaire l'information des personnes dans le cas des traitements intéressant la Sûreté, la Défense ou la Sécurité publique ou ayant pour objet l'exécution de condamnations pénales ou de mesures de sûreté.

Ainsi, pour le fichier de renseignement de la direction centrale de la Sécurité intérieure, cristina, l'obligation d'information n'existe pas. Il en est de même pour les fichiers d'antécédents judiciaires. Ainsi, en 2006, lors des travaux du Groupe de travail sur l'amélioration du contrôle des fichiers de police et de gendarmerie, la cnil remarquait qu'aucune mesure d'information n'avait été prévue à l'égard des personnes mises en cause et enregistrées dans les fichiers stic et judex. Tout en reconnaissant ce droit reconnu par la loi, elle indiquait que, dès lors que ces fichiers de police judiciaire étaient utilisés à des fins administratives et dans le cadre d'enquêtes liées à des demandes d'emploi, l'information des personnes sur l'existence et les conditions d'exercice de ses droits, ainsi que sur leur droit d'accès, devait être reconnue et garantie par des mesures spécifiques telles que l'affichage dans les locaux des commissariats, des mentions sur les dépôts de plaintes, etc. Le ministère de l'Intérieur reste très attaché à l'application du droit actuel, confirmé par le législateur en 2004 après avis de la cnil sur le projet de loi créant le stic, et qui tient compte de la spécificité des fichiers de police. Il considère ainsi qu'informer systématiquement les personnes mises en cause que des informations les concernant sont conservées dans les fichiers de police judiciaire serait de nature à alourdir considérablement la procédure. Par ailleurs, dans certaines enquêtes, cela serait impraticable sauf à mettre en péril leur efficacité. Une inscription dans le stic ne découle pas nécessairement d'un placement en garde à vue et celle-ci est légitime dès lors qu'il existe des indices graves ou concordants, qui peuvent être réunis sur la base d'informations obtenues auprès de tiers, par exemple des

mis en cause complices, ou encore des témoins, ou encore sur la base d'indices matériels. Un « droit à l'information » pourrait compromettre certaines enquêtes, conduire à la destruction de preuves ou entraîner la fuite des auteurs mis en cause.

En revanche, une information sur le fait qu'une consultation des fichiers de police pourra être mise en œuvre est systématiquement délivrée, dans le récépissé de demande, à toute personne sollicitant une décision administrative impliquant une enquête administrative pouvant donner lieu à consultation de fichiers.

Pour les victimes, qui sont également enregistrées dans ces fichiers, une procédure d'information a été mise en œuvre en application du décret créant le stic. Ce droit à l'information a été mis en œuvre par affichage (modification de la charte d'accueil du public et d'assistance aux victimes, art. 8), complété par une notice explicative et détaillée, document précisant l'étendue de ce droit et ses modalités d'exercice (mise à disposition de modèles de courrier à l'attention de la cnil, du procureur de la République ou du service régional gestionnaire de la documentation).

Dans la version du décret transmis à la cnil, en novembre 2008, le pouvoir exécutif a expressément prévu de ne pas appliquer le droit d'information aux données enregistrées dans le fichier edvrisp.

2. Le droit d'opposition

L'article 38 de la loi de 1978 permet à toute personne de s'opposer, pour des motifs légitimes, à ce que des données à caractère personnel la concernant fassent l'objet d'un traitement, sauf dans les cas où le traitement répond à une obligation légale ou lorsque l'application de cette règle a été écartée par des dispositions expresses. La loi de 2004 consacre le droit de s'opposer, sans frais, à l'utilisation de ses données à des fins de prospection, notamment commerciale.

Pour la très grande majorité des fichiers de police et de gendarmerie, le droit d'opposition ne s'applique pas. Pour les fichiers stic et judex, le droit d'opposition existe pour les victimes qui peuvent s'opposer à ce que des données à caractère personnel la concernant soient conservées dans le fichier dès lors que l'auteur des faits a été condamné définitivement.

3. Le droit d’accès

Il existe deux types de droit d’accès aux données. L’un est direct et l’autre indirect. En principe, toute personne peut demander et obtenir communication des données la concernant enregistrées dans un fichier. Une copie des données à caractère personnel est délivrée à l’intéressé à sa demande. Le droit accès est exclu lorsque les données sont conservées sous une forme excluant manifestement tout risque d’atteinte à la vie privée et aux seules fins de statistiques ou de recherche scientifique ou historique.

Pour les fichiers intéressant la sûreté de l’État, la Défense et la Sécurité publique, le droit d’accès est indirect. Toute personne qui souhaite exercer son droit d’accès doit s’adresser à la cnil qui désigne l’un de ses membres, appartenant ou ayant appartenu au Conseil d’État, à la Cour de cassation ou à la Cour des comptes, pour mener toutes investigations utiles. Le commissaire exerce, en lieu et place du demandeur, le droit d’accès, de rectification ou d’effacement des données soit inexactes, soit collectées ou conservées en contradiction avec la loi.

Depuis la loi du 18 mars 2003, lorsque la Commission constate, en accord avec le responsable du traitement, que la communication des données ne met pas en cause les finalités du traitement, la sûreté de l’État, la Défense ou la Sécurité publique, les données peuvent être transmises au requérant. Préalablement à l’entrée en vigueur de cette loi, la Commission ne pouvait que notifier à l’intéressé qu’il avait procédé aux vérifications demandées. Elle ne pouvait communiquer les données sauf dans le cas prévu par le décret du 14 octobre 1991 créant l’ancien fichier des renseignements généraux.

Certains fichiers de police sont soumis au droit d’accès direct. Ainsi, la cnil, suite à l’interprétation de la notion de « sécurité publique », a considéré que le droit d’accès direct devait être appliqué au fichier national des empreintes digitales, car les informations enregistrées revêtaient un caractère strictement objectif et que leur transmission ne pouvait donc pas porter atteinte à la sécurité publique [8]. Ce même droit a été ménagé pour le fichier national des empreintes génétiques.

Les demandes de droit d’accès indirect visent principalement les fichiers stic et judex, notamment suite à une décision défavorable prise après enquête

administrative, et, depuis l'affaire Bruno Rebelle [9] de mars 2007, l'ancien fichier des renseignements généraux. C'est majoritairement parce qu'un citoyen conteste une décision prise après consultation des fichiers qu'il demande à accéder aux fichiers, en préalable, et/ou en parallèle, à un recours hiérarchique.

La procédure est complexe, donc souvent longue, d'autant plus si le requérant a fait l'objet de multiples inscriptions dans des ressorts juridictionnels différents. Elle nécessite l'intervention, outre de la cnil, d'autant de services de police et d'autant de parquets qu'il y a d'inscriptions relatives à des affaires commises dans des ressorts différents.

Très souvent, le public distingue mal l'exercice des droits d'accès aux fichiers de police prévus par les articles 41 et 42 de la loi Informatique et Libertés, de l'exercice d'un recours contre une décision préfectorale négative. Ainsi, il est fréquent que des personnes sollicitent l'effacement des données les concernant à titre d'« indulgence » en indiquant regretter des « erreurs passées » ou des « erreurs de jeunesse » alors même qu'elles reconnaissent avoir commis des actes délictuels. Elles s'adressent alors à une autorité incompétente, l'autorité administrative, souvent préfectorale, alors que la loi dispose que le traitement des données nominatives contenues dans le stic ou judex s'exerce sous le contrôle du procureur de la République.

Par ailleurs, l'exercice du droit d'accès indirect se heurte aux délais parfois très importants pour obtenir communication des données. Or, le décret du 20 octobre 2005 pris pour l'application de la loi du 6 janvier 1978 modifiée prévoit, en son article 87, que la cnil doit notifier au demandeur le résultat de ses investigations dans un délai de quatre mois à compter de sa saisine. Ce texte prévoit aussi que le responsable du traitement dispose, pour réaliser ses investigations, d'un délai de trois mois à compter de la transmission de la demande de droit d'accès par la Commission. Ce délai ne suspend pas celui de quatre mois qui s'impose à la cnil. Les modalités actuelles d'instruction des demandes par le ministère de l'Intérieur et la lenteur des réponses des parquets ne permettent pas à la cnil de respecter les termes de l'article 87 du décret.

L'exercice du droit d'accès a été assoupli par la jurisprudence administrative en 2002 suite au recours de M. Moon [10]. Ainsi, le juge administratif s'est considéré compétent pour apprécier le caractère communicable ou non communicable des informations contenues dans un fichier. En cas de recours, l'administration doit établir que la communication des informations au requérant

serait de nature à porter atteinte à la sûreté de l'État, la Défense et la Sécurité publique. Toutefois, la loi du 6 août 2004 confirme les principes édictés sous l'empire du précédent texte, même s'il est désormais prévu que la cnil peut constater, en accord avec le responsable du fichier, que la communication des données qui y sont contenues ne met pas en cause ses finalités, entraînant la possibilité pour le requérant d'obtenir communication des informations. Ce texte vient donc consacrer la position de la cnil et la jurisprudence du Conseil d'État. Reste à savoir si ce droit d'accès direct aux données ne sera possible que si l'acte réglementaire créant le fichier le prévoit ou, dans tous les cas, et cela, dès l'instant où les critères de la jurisprudence Moon sont respectés.

En 2008, la cnil a reçu 1 057 demandes de droit d'accès indirect aux fichiers stic et judex contre 1 475 en 2007. Les demandes relatives au fichier des renseignements généraux se sont élevées à 1 038 en 2008 contre 1 607 en 2007. En revanche, celles concernant le fichier tenu par l'ex-direction de la Surveillance du territoire sont passées de 93 en 2007 à 264 en 2008. Le débat suscité par la publication des deux décrets portant création des fichiers edvige et cristina, suite à la réforme des services de renseignement, a sûrement contribué à cette augmentation des demandes portant sur l'accès aux informations enregistrées dans le fichier de renseignement jusque-là géré par la dst et peu connu de l'opinion.

4. Le droit de rectification

Le droit de rectification est garanti par les textes internationaux et notamment par la convention 108 du Conseil de l'Europe. Il figure à l'article 40 de la loi du 6 janvier 1978 qui dispose que toute personne peut demander que soient rectifiées, complétées, mises à jour ou effacées les données la concernant qui sont inexactes, incomplètes, équivoques, périmées ou dont la collecte, l'utilisation ou la conservation est interdite. Si des modifications sont apportées, le responsable du traitement devra justifier les opérations effectuées et délivrer une copie de l'enregistrement modifié.

Pour les fichiers de police, la rectification ou l'effacement de données s'exerce par l'intermédiaire de la cnil ou du procureur de la République. Il est le pendant du droit d'accès. Toutefois, étant donné que les intéressés n'ont pas toujours connaissance du détail des informations enregistrées, ils ne sont pas en mesure de les contester et donc de les rectifier. Les commissaires de la cnil ne pourront

que demander la suppression des informations dont la collecte est illégale ou pour lesquelles la durée de conservation est dépassée. Le droit de rectification exercé par la cnil suite à des informations erronées n'est donc possible que dans les cas où les données enregistrées ont pu être transmises (ou connues) au requérant.

Par ailleurs, les décrets portant création des traitements stic et judex ont ménagé un droit de rectification auprès du procureur de la République. Il est ainsi prévu de permettre à la personne fichée de s'adresser directement au parquet qui a en charge le contrôle du fichier. Toute personne mise en cause peut demander directement au procureur de la République, en cas de décision de non-lieu, de relaxe ou d'acquittement, de mettre à jour le fichier. Il est également possible d'exiger que la qualification initiale enregistrée dans le fichier soit remplacée par la qualification des faits finalement retenue par l'autorité judiciaire.

Lors de ses travaux en 2006, le Groupe de travail sur le contrôle des fichiers de police s'est interrogé sur la nécessité de prévoir une voie de recours contre les décisions du parquet en matière de conservation ou d'effacement des données. Cette position était notamment soutenue par le médiateur de la République qui voyait, dans la décision du procureur de ne pas donner suite à une demande d'effacement, une décision faisant grief susceptible d'un recours. La chancellerie estimait, quant à elle, que le contrôle du procureur de la République, opéré à l'occasion de l'exercice du droit d'accès indirect, quelles qu'en soient ses modalités, avait pour objet de déterminer si les mentions figurant dans les fichiers stic et judex, si elles existent, répondent lors de la demande aux conditions légales pouvant conduire à leur effacement ou à leur rectification. Par conséquent, elle jugeait que, si les conclusions du magistrat sur le mérite de certaines données à être rectifiées ou effacées sont adressées au responsable du traitement, celui-ci demeurait donc la seule autorité compétente, à l'exclusion de toute autre, pour prendre ou non la décision d'effacement ou de rectification et la notifier au requérant. Le procureur de la République peut ainsi porter ses conclusions à la connaissance du requérant à titre de simple mesure d'information, afin d'attester de l'effectivité de son contrôle sur les mentions enregistrées au stic. Pour autant, cette information, matérialisée par le courrier du procureur de la République, ne faisant pas grief au demandeur, elle serait insusceptible de recours quelle qu'en soit sa nature. Cette demande n'avait pas fait l'objet d'un consensus et avait été rejetée. Elle a été renouvelée lors du second rapport sur les fichiers en décembre 2008, le groupe de contrôle recommandant, *a minima*, la mise en place d'une procédure de notification à

l’intéressé par le service gestionnaire du fichier dès lors que la décision de maintien de son inscription dans les fichiers d’antécédents judiciaires serait prise sur prescription du parquet.

La loi du 18 mars 2003 a créé un droit de rectification auprès du procureur de la République au bénéfice des personnes dont les profils génétiques sont inscrits dans le fnaeg. Une telle demande serait possible dès lors que la conservation n’apparaîtrait plus nécessaire au regard de la finalité du fichier. Si le procureur refuse de faire droit à la demande, il est alors possible de saisir le juge des libertés et de la détention dont la décision pourra aussi être contestée devant la chambre d’instruction [11].

VII. Un encadrement croissant par la technique elle-même

Le droit prend en compte les caractéristiques spécifiques des fichiers de police et de gendarmerie puisque la loi du 6 janvier 1978 réserve un cadre particulier aux fichiers qui « intéressent la sûreté de l’État, la Défense ou la Sécurité publique », ou qui « ont pour objet la prévention, la recherche, la constatation ou la poursuite des infractions pénales ». Ce statut particulier réservé aux fichiers de police est d’ailleurs consacré par la directive européenne 95/46.

Les limites imposées à l’usage des traitements de données sont d’abord liées au principe fondamental de la segmentation des bases de données, profondément enraciné dans la législation « Informatique et Libertés » française. L’éclatement des réseaux entre les opérateurs concourant à la réalisation d’une seule opération de communication électronique, par exemple, constitue une limitation drastique des possibilités d’accès aux informations nominatives. L’interdiction des interconnexions des fichiers, expressément mentionnée dans l’ensemble des textes créant les fichiers, est une garantie supplémentaire.

Par ailleurs, si l’informatique permet un accès facilité, démultiplié et instantané à des bases d’informations nominatives, sont aussi enregistrées en mémoire des traces de chaque consultation, ce qui n’était et n’est pas le cas lorsque les fichiers sont manuels.

Le progrès informatique sécrète donc de manière endogène les outils permettant

de mieux encadrer l'utilisation des fichiers. Aujourd'hui, grâce à l'informatique, il est possible de tracer la personne qui consulte une base de données et ainsi contrôler le respect par les policiers du cadre de leur mission. La consultation de la grande majorité des fichiers de police s'effectue désormais par une interface d'accès qui journalise accès et consultation de manière individualisée, par poste et par agent : elle est désignée par l'acronyme cheops.

La traçabilité fait et fera l'objet de perfectionnements au fur et à mesure de la révision de l'architecture technique des applications. La sécurisation de l'accès et de la consultation des fichiers de police passera à l'avenir inéluctablement par l'usage de techniques comme la biométrie digitale ou oculaire.

C'est notamment grâce à l'accroissement des opportunités offertes par la traçabilité que les dérives individuelles de quelques fonctionnaires de police, se servant de leur accès au stic pour vendre les informations à des entreprises privées ou à des journalistes, pourront être suivies plus efficacement. Cela implique nécessairement que des contrôles systématiques soient effectués et que des systèmes d'alerte automatique soient mis en place afin d'éviter, comme l'indique la cnil dans son rapport de janvier 2009, que « si la traçabilité des accès et des connexions au stic est techniquement possible, cette fonction de contrôle ne soit pratiquement jamais utilisée (seulement 120 contrôles en 2008) ».

Il convient aussi de s'assurer que les consultations du stic à des fins administratives soient systématiquement effectuées à partir du module de police administrative et non, comme cela semble être le cas la plupart du temps, à partir du module de police judiciaire [12]. Comme l'indique la cnil, actuellement, les mesures adoptées par le ministère de l'Intérieur pour encadrer les consultations du stic à des fins administratives ne sont pas appliquées au sein des services de police faute de contrôle hiérarchique et organisé.

À plusieurs reprises, le Groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie a souhaité la mise en place d'un système d'alerte automatique pour certains fichiers (notamment ceux d'antécédents et de renseignements) en cas de surconsultation d'un dossier ou dans le cas d'un agent qui consulterait un trop grand nombre de dossiers.

VIII. Les problèmes de mise à jour et

d’erreurs

Les craintes et les doutes suscités par les fichiers de police et de gendarmerie font généralement suite, soit à la création ou à la mise à jour d’un nouveau traitement, comme cela a été le cas lors de la publication du décret portant création d’edvige, soit à des dysfonctionnements liés à l’utilisation de données d’un fichier lors des enquêtes administratives.

Dans le premier cas, le débat porte principalement sur le développement accru des fichiers de police, la proportionnalité de leurs finalités ou de leurs possibilités au regard de la protection des libertés et du droit à la vie privée. Il s’agit donc de questions philosophiques, voire juridiques, sur les limites que doit s’imposer l’État dans le cadre de la modernisation et du développement de systèmes de traitement de l’information ayant pour finalité la protection de la sécurité de la population et la sûreté de l’État.

Suite à la possibilité d’utiliser les fichiers d’antécédents judiciaires dans le cadre des enquêtes administratives et, malgré le contrôle de la cnil, les diverses modifications législatives intervenues en vue d’améliorer l’encadrement de ces fichiers et les opérations d’apurement importantes réalisées par les services de police et de gendarmerie, certains dysfonctionnements susceptibles de porter atteinte aux libertés individuelles sont apparus.

Concernant l’utilisation des fichiers des services de renseignements, dans lesquels prédominent les éléments « qualitatifs », dans le cadre des enquêtes administratives, la jurisprudence administrative a clairement fixé les règles, qu’il s’agisse de décisions relatives au droit au séjour des étrangers ou même à des refus d’habilitation ou d’agrément. C’est le cadre fixé par cette jurisprudence qui est, par exemple, appliqué dans le dossier de la sécurité aéroportuaire.

– Application du cadre législatif de la loi n° 79-587 du 11 juillet 1979 (motivation des actes administratifs) : la motivation est obligatoire pour « les décisions qui restreignent l’exercice des libertés publiques ou, de manière générale, constituent une mesure de police », qui « infligent une sanction, ou retirent ou abrogent une décision créatrice de droits ».

– En cas de procédure contentieuse, la motivation peut être étayée par une note des services de renseignement établie à partir des informations conservées par

les services dans leurs fichiers. Cette note est reconnue par le juge comme ayant une valeur probante sous la condition qu'elle soit suffisamment précise et circonstanciée. Toutefois, cette valeur probante n'est pas automatique et le magistrat examine tous les éléments qui lui sont apportés par le requérant (ce, 3 mars 2003, ministère de l'Intérieur contre Rakhimov).

Enfin, il y a la situation du stic et de judex, deux fichiers alimentés quasiment en temps réel par les officiers de police judiciaire lorsqu'ils transmettent les conclusions de leurs enquêtes au magistrat compétent, procureur ou juge d'instruction. Les données enregistrées résultent de l'appréciation des faits par l'opj qui les qualifie. Mais cette qualification peut être complétée, réformée ou infirmée par l'autorité judiciaire, aussi bien par le procureur de la République, le juge d'instruction que par la juridiction de jugement. C'est notamment à l'occasion de cette requalification ou aux décisions prononcées par les juridictions que les principaux problèmes peuvent se poser. C'est d'ailleurs ce qui avait été principalement relevé par le Groupe de travail sur les fichiers de police et de gendarmerie en 2006 et par la cnil lors d'une importante opération de contrôle en 2008.

La mise en place d'un groupe de contrôle sur les fichiers

Par lettre de mission du 15 juin 2006, le ministre d'État, ministre de l'Intérieur et de l'Aménagement du territoire a demandé à Alain Bauer, président du Conseil d'orientation de l'Observatoire national de la délinquance, de mettre en place un groupe de travail en vue d'améliorer le contrôle et l'organisation des fichiers de police et de gendarmerie afin d'éviter le maintien d'informations erronées ou dépassées. Ce Groupe de travail, composé des administrations (Intérieur, Défense, Justice), de syndicats de police et de magistrats, de la cnil, du médiateur de la République de la cnds, a remis son rapport le 15 novembre 2006. Les différentes recommandations du groupe de travail ont porté sur le renforcement des garanties individuelles visant à s'assurer que des informations non actualisées, inexactes ou dont la date de validité de conservation a expiré soient écartées des fichiers et ne risquent plus ainsi de nuire à l'employabilité des personnes. Elles ont également visé à rappeler que les décisions préfectorales, prises après consultation du stic ou du fichier judex, devaient faire l'objet d'une véritable instruction, prenant en compte la gravité, la répétition et l'ancienneté des faits. L'ensemble des recommandations du groupe de travail

avait été approuvé par le ministère de l'Intérieur.

En septembre 2008, suite notamment aux polémiques suscitées par la publication du décret portant création du fichier edvige, le groupe de travail a été réactivé par le ministère de l'Intérieur. Sa composition a été élargie à certaines associations (licra, sos racisme, sos homophobie) et aux représentants des avocats. Un nouveau recensement des fichiers existant ou à venir a été réalisé. Les suites des recommandations du rapport 2006 ont été listées et près de 25 nouvelles recommandations ont été faites dans un rapport rendu au ministre de l'Intérieur en décembre 2008.

Un arrêté du 20 octobre 2009 a porté création officielle d'un groupe de travail sur l'amélioration du contrôle et de l'organisation des bases de données de police. « Le groupe de travail adresse au ministre de l'Intérieur des orientations et recommandations sur les conditions générales de création et d'utilisation des fichiers de police et de gendarmerie et sur la cohérence d'ensemble du développement de ces fichiers, au regard des évolutions technologiques et des contraintes opérationnelles. Il assure à intervalles réguliers un recensement de ces fichiers. Il peut être saisi par le ministre de toute question relative à ce domaine. » (art. 2.)

1. La durée de conservation des données

Les textes réglementant le stic et judex prévoient que les données enregistrées ne peuvent être conservées que durant une certaine durée. Les informations doivent donc être effacées automatiquement dès lors qu'elles n'ont plus à figurer dans le fichier. Une partie des erreurs relevées par la cnil lorsqu'elle a été saisie par une personne mise en cause provient notamment du maintien d'informations qui auraient dû être effacées. Depuis la mise en œuvre des programmes d'apurement des données dans le stic et dans judex, des milliers de fiches ont été mises à jour. Conséquemment, le nombre de rectifications en raison du délai de conservation expiré a chuté depuis fin 2004. Il tient désormais pour l'essentiel à l'incidence de la requalification pénale des faits (délits requalifiés en faits contraventionnels de 5e classe) entraînant une correction dans la durée de conservation des informations criminelles (passage d'une durée de vingt ans à cinq ans). Désormais, les données dont la durée de conservation arrive à expiration dans le

mois en cours sont effacées automatiquement.

Suite à la mise en place du logiciel d'apurement de judex (datepur), 55 716 fiches personnes ont été supprimées en 2006, 72 026 en 2007 et 79 641 en 2008.

2. La mise à jour des données

La majorité des erreurs relevées par la cnil lors de ses contrôles porte sur les questions relatives à la mise à jour des données. Les dysfonctionnements sont d'abord liés à l'absence d'une procédure de transmission régulière par les parquets des suites judiciaires favorables au gestionnaire du stic ou de judex.

C'est notamment ce que relevait la cnil dans un rapport rendu en janvier 2009, confirmant les conclusions du groupe de travail sur les fichiers de police et de gendarmerie de 2006, et portant sur un contrôle du stic [13]. Elle constate ainsi, entre autres, « une absence quasi systématique de transmission par les parquets des suites judiciaires nécessaires à la mise à jour du stic (classements sans suite, acquittements, décisions de non-lieu, requalifications pénales) » ou encore le fait que, « dans certains cas, des demandes d'effacement sont formulées mais elles ne sont pas prises en compte par le ministère de l'Intérieur ».

S'agissant des autres motifs (problème de requalification de l'infraction, infraction non constituée, enregistrement à tort comme mis en cause, absence d'archive), ils semblent relever à la fois d'erreurs de saisie à la source et du contrôle insuffisant des parquets ou des autorités hiérarchiques, notamment les chefs de service, sur le contenu des fiches stic et judex. Le fait que les parquets ne disposent pas de terminaux d'accès au stic ou à judex leur permettant en temps réel de vérifier le contenu des fiches, de procéder notamment à la requalification des faits, constitue un obstacle à l'exercice effectif de leur contrôle.

Les textes réglementant les traitements stic et judex prévoient que la mise à jour des fichiers au regard des suites judiciaires relève de la compétence du procureur de la République territorialement compétent qui doit transmettre au gestionnaire du fichier certaines décisions de justice n'ayant pas donné lieu à poursuites ou à condamnations.

L'article 21. III de la loi du 18 mars 2003 relative à la sécurité intérieure précise

les suites judiciaires donnant lieu à la mise à jour des données à caractère personnel inscrites dans les fichiers de police judiciaire dits d'antécédents. Il s'agit d'une part, des décisions de relaxe et d'acquittement devenues définitives qui doivent donner lieu à l'effacement des données enregistrées, sauf si le procureur en ordonne le maintien pour des raisons liées aux finalités du fichier (ex. : cas de relaxe motivée sur le fondement de l'article 122-1 du Code pénal). Il s'agit d'autre part des décisions de classement sans suite pour insuffisances de charges et de non-lieu qui doivent compléter les données inscrites dans les fichiers par l'apposition d'une mention sauf si le procureur de la République en prescrit l'effacement. Le champ des suites judiciaires donnant lieu à la mise à jour ou à l'effacement des données enregistrées est bien moins large que celui des décisions prises par les procureurs de la République qui n'aboutissent pas à la mise en œuvre de l'action publique ou à des condamnations.

En pratique, la transmission de ces informations ne s'opère pas de façon immédiate et systématique et certains parquets ont des difficultés pour mettre en œuvre cette procédure de manière optimale.

Afin de pallier partiellement ce défaut lié à la transmission des données mises à jour, et à l'occasion de l'examen du décret portant création du stic, la cnil, « tout en prenant acte que le projet de décret prévoit que la consultation du fichier à des fins administratives ne peut porter ni sur les données relatives aux victimes ni sur les données concernant des personnes mises en cause ayant fait l'objet d'une mise à jour ordonnée par le procureur de la République, […] estimait toutefois que des dispositions devaient être prévues afin que le résultat de la consultation ne puisse être communiqué à l'autorité compétente qu'après que le responsable du fichier s'est assuré auprès du procureur de la République compétent qu'aucune décision judiciaire n'est intervenue qui appellerait la mise à jour de la fiche de l'intéressé ou encore qu'aucune requalification judiciaire n'est intervenue qui justifierait la rectification des informations figurant sur cette fiche ».

Cette proposition de la cnil n'a pas été retenue par le Gouvernement, car elle aurait conduit, tout d'abord, à faire intervenir une autorité judiciaire, le procureur de la République, dans le cours d'une enquête administrative et lui conférer un pouvoir d'intervention, puis aurait abouti au prolongement des délais de réponse aux intéressés, voire de blocage de la procédure administrative en cas de silence du procureur de la République.

Si l’accès aux fichiers, par l’implantation de terminaux de consultation dans les juridictions, peut être utile au contrôle exercé par le procureur de la République sur les données enregistrées, il n’en reste pas moins que l’autorité judiciaire ne pourra être en mesure de faire face à ses obligations que, quand elle aura à disposition un outil lui permettant d’assurer une transmission automatisée des suites judiciaires concernées aux gestionnaires des fichiers. Le système Cassiopée [14], qui est en cours de déploiement dans les juridictions (il devrait être intégralement déployé en 2012), autorisera une telle transmission dans l’application Traitement des procédures judiciaires.

Un groupe de travail technique tpj-Cassiopée a été constitué dans le cadre général des échanges de données contenues dans les procédures pénales entre les services d’enquêtes et les tribunaux (afin notamment d’assurer le continuum statistique) et dans le cadre plus particulier de la préparation de la mise à jour automatisée des fichiers de police judiciaire. Il se réunit régulièrement depuis juillet 2006, mais le calendrier des développements informatiques, de part et d’autre, ne permettra pas un début de réalisation concrète avant mi-2011.

3. La requalification judiciaire des faits

Des rectifications dans le stic peuvent également avoir pour origine des enregistrements infondés ou devenus sans fondement à la suite d’une requalification judiciaire des faits.

Outre les inscriptions devenues sans fondement en raison d’une requalification « à la baisse » des faits ou d’une mesure de classement en raison de l’insuffisance de charges ou du caractère insuffisamment caractérisé de l’infraction, une part des anomalies relevées trouve son origine dans une insuffisance de la qualité de rédaction des comptes rendus d’enquête après identification (crei.), indispensables à l’alimentation et à la gestion du stic et qui peuvent parfois présenter des inexactitudes et/ou imprécisions au regard des mentions portées dans la procédure qu’ils accompagnent.

Il appartient donc à l’opérateur de saisie chargé de l’enrichissement du stic et au procureur de la République (rendu destinataire du crei., en même temps que de la procédure) dans son pouvoir de contrôle du fichier, de vérifier les informations inscrites sur le crei. L’exactitude des mentions est toutefois rarement vérifiée à ce stade.

De même, la mise en œuvre concomitante de Cassiopée et du système tpj (2011-2012), qui instaurera une transmission informatique directe des données contenues dans les procédures pénales depuis le service d'enquête vers le bureau d'ordre pénal du tribunal de grande instance, les suites judiciaires étant quant à elles transmises en retour par la même voie, assurera une réelle mise à jour systématique des fichiers d'antécédents judiciaires.

IX. La nécessité d'un meilleur contrôle…

L'équilibre nécessaire entre protection des libertés individuelles et collectives, et sûreté de la population et de l'État, nécessite un compromis ordonné et précis. La reconquête du pôle de défense des libertés a commencé en 1974, s'est affirmée en 1978, et a connu une forte accélération à l'occasion de la courageuse décision de Michel Rocard, alors Premier ministre, de sortir de la clandestinité les fichiers des Renseignements généraux et de la direction de la Surveillance du territoire.

Depuis 2006, et la mise en place du groupe de travail sur les fichiers de police par Nicolas Sarkozy, alors ministre de l'Intérieur, réactivé en 2008 par Michèle Alliot-Marie sous la forme d'un groupe de contrôle des fichiers de police et de gendarmerie, et officialisé par Brice Hortefeux en novembre 2009, les questions posées ont rencontré un vif écho au sein de l'opinion publique et des associations de défense des libertés.

L'affaire « edvige » a montré qu'on ne pouvait plus transposer un fichier ancien (celui des Renseignements généraux dans ce cas), dans des conditions de rédaction parfois critiquables, sans assurer en même temps une dynamique d'amélioration des garanties de contrôle des fichiers par des autorités judiciaires et/ou indépendantes.

Les récents rapports de la cnil, mettant en exergue certaines erreurs contenues dans le fichier stic susceptibles de porter atteinte aux libertés individuelles, ne font que confirmer l'importance qui doit être accordée à la modernisation des bases de données mais, surtout, au nécessaire contrôle dont celles-ci doivent faire l'objet.

Par ailleurs, de nombreux domaines de l'investigation technique vont connaître des changements majeurs grâce au progrès du traitement et données massives mais aussi au développement important et rapide de l'informatique et de la science. Les systèmes d'information fonctionneront bientôt sans données structurées à l'exemple des moteurs de recherche sur Internet. Les dispositifs d'encadrement juridique de l'activité policière devront donc être revus et les dispositions de la loi de 1978 adaptées.

En mars 2009, un rapport d'information parlementaire sur les fichiers de police a été rendu par les députés Delphine Batho et Jacques Alain Bénisti suite aux travaux conduits par la commission des lois dans le cadre des débats sur le fichier de renseignement « edvige ». Certaines recommandations issues de ce rapport ont débouché sur une proposition de loi [15] visant à mieux encadrer la création et le développement des fichiers notamment en proposant que tout traitement de données à caractère personnel qui intéresse la sécurité publique ou qui a pour objet la prévention, la recherche, la constatation ou la poursuite d'infractions pénales ou l'exécution des condamnations pénales ou des mesures de sûreté soit autorisé par la loi et non plus par acte réglementaire.

La loppsi a également renforcé l'encadrement juridique des principaux fichiers de police judiciaire dont ceux liés à l'analyse sérielle.

Les ministères de l'Intérieur, de la Défense mais également de l'Économie vont également devoir se doter des moyens internes de contrôle tant dans le domaine technique, lié notamment à la mise en place des contrôles biométriques, qu'humain avec le renforcement des missions d'inspection mais également celles relatives au contrôle hiérarchique. L'annonce par le ministère de l'Intérieur, en janvier 2009, de la mise en place d'un service dédié au contrôle des fichiers au sein de l'inspection générale de l'administration va dans ce sens.

De même, les deux directions générales de la Police et de la Gendarmerie nationales ont entamé une démarche visant à renforcer les contrôles et les procédures relatifs aux bases de données. Les formations initiales et continues des fonctionnaires ont été renforcées. Un guide « Théorie et pratique des fichiers de police » a été rédigé et diffusé par la dgpn. De même, cette dernière a créé un réseau de 200 conseillers informatique et libertés (cil) ayant notamment pour mission de mieux identifier les besoins locaux en matière de traitements automatisés, de s'assurer qu'aucun traitement local n'échappe à un encadrement juridique, d'assister les services dans l'élaboration des déclarations et de

favoriser les échanges d'expériences. De son côté, la direction générale de la Gendarmerie nationale a mis en place 10 référents centraux informatique et libertés et 30 référents territoriaux. Un bureau de contrôle des fichiers a également été créé à l'Inspection générale de la Gendarmerie nationale.

Le groupe de travail sur l'amélioration du contrôle et de l'organisation des fichiers de police et de gendarmerie, très majoritairement composé de personnalités indépendantes du gouvernement, a émis de nombreuses recommandations en vue d'améliorer les garanties accordées au citoyen. Il a également suggéré des mesures sur la protection des mineurs, l'accélération des mises à jour ou encore le contrôle des fichiers de renseignement. Il est désormais saisi préalablement de tout projet visant à créer de nouvelles bases de données.

D'autres administrations, notamment à Bercy (direction générale des Douanes et des Droits indirects) ou au ministère de la Justice et des Libertés, se sont engagées dans le même mouvement consistant à recenser l'existant, à exhumer ce qui était caché ou oublié et à détruire, dans le respect de la législation sur les archives, ce qui était devenu inutile ou obsolète.

Ce processus de confiance nécessite d'importants efforts de la part des administrations et un outil de contrôle préalable à la création de nouveaux fichiers ou de nouvelles applications informatiques afin d'éviter les dérapages et les incompréhensions.

C'est à ce prix seulement que notre démocratie pourra se protéger sans se renier.

Tableau récapitulatif des principaux fichiers

Notes

[1] Décision n° 91-294 DC du 25 juillet 1991.
[2] Décision n° 2003-467 DC du 13 mars 2003.
[3] Décision n° 2004-492 DC du 2 mars 2004.
[4] Décision n° 92-316 DC du 20 janvier 1993.
[5] Décision n° 2004-499 DC du 29 juillet 2004.

[6] Voir le chap. I. 1 : « Qu'est-ce qu'un fichier? »
[7] La cnil a ainsi jugé déloyale la collecte d'informations sur la solvabilité d'une personne en s'adressant à son insu au syndic ou au concierge de l'immeuble d'habitation. Elle a également qualifié de déloyale la collecte indirecte opérée par la Gendarmerie nationale s'adressant à des tiers à l'insu de l'intéressé (3e rapport annuel de la cnil).
[8] Délibération nº 86-102 du 14 octobre 1986.
[9] La diffusion de la fiche des renseignements généraux de Bruno Rebelle, ancien président de Greenpeace France et membre de l'équipe présidentielle de Ségolène Royal, avait suscité une vive polémique en mars 2007. Le Parti socialiste avait accusé Nicolas Sarkozy, alors ministre de l'Intérieur, d'enquêter sur l'équipe de sa concurrente à l'élection présidentielle. Un officier de la direction centrale des renseignements généraux (dcrg) suspecté d'avoir remis à la presse la fiche confidentielle concernant Bruno Rebelle a été mis en examen et placé sous contrôle judiciaire le 11 mai 2007.
[10] Conseil d'État, Ass. 26 novembre 2002, Moon.
[11] Art. R. 53-13-1 et R. 53-13-2 du Code de procédure pénale.
[12] Le profil judiciaire permet d'accéder, si la personne est connue, à l'ensemble des informations enregistrées dans le stic. En revanche, le profil administratif ne permet d'avoir accès qu'aux seules affaires auxquelles aucune suite judiciaire favorable à l'intéressé (telles que classement sans suite pour insuffisance de charges, relaxe, acquittement, non-lieu) n'a été donnée par l'autorité judiciaire.
[13] Ce rapport a été réalisé suite à 19 contrôles sur place de juin 2007 à novembre 2008 (7 commissariats de police, 4 services régionaux de police judiciaire, 4 tribunaux de grande instance, 3 préfectures, 1 direction régionale des renseignements généraux) ; un questionnaire adressé aux 34 tribunaux de grande instance les plus importants de France (qui représentent 50 % de l'activité pénale) ; questionnaires techniques adressés au ministère de l'Intérieur.
[14] Cassiopée est le nom du futur système de traitement des données du ministère de la Justice.
[15] Proposition de loi relative aux fichiers de police nº 1659, 7 mai 2009.